



REX300

Ethernet-Router mit MPI/PROFIBUS

700-87X-XXX02

Handbuch

Ausgabe 3 / 01.05.12 ab FW 3.0.4 und Geräte mit der Bestellnummernendung 02
Handbuch Bestellnummer : 900-87x-REX300

Systeme Helmholz GmbH | Hannberger Weg 2 | 91091 Großenseebach

Fon: +49 9135 7380-0 | Fax: +49 9135 7380-110 | E-Mail: info@helmholz.de | Internet: www.helmholz.de

***Systeme Helmholz* GmbH**

Hannberger Weg 2, 91091 Großenseebach

Hinweis:

Der Inhalt dieses Handbuches ist von uns auf die Übereinstimmung mit der beschriebenen Hard- und Software überprüft worden. Da dennoch Abweichungen nicht ausgeschlossen sind, können wir für die vollständige Übereinstimmung keine Gewährleistung übernehmen. Die Angaben in diesem Handbuch werden jedoch regelmäßig aktualisiert. Bitte beachten Sie beim Einsatz der erworbenen Produkte jeweils die aktuellste Version des Handbuchs, die im Internet unter www.helmholz.de einsehbar ist und auch heruntergeladen werden kann.

Unsere Kunden sind uns wichtig. Wir freuen uns über Verbesserungsvorschläge und Anregungen.

Änderungen in diesem Dokument:

Stand	Datum	Änderung
1	19.05.2010	Erstausgabe
2	28.10.2010	Änderungen wegen neuer Firmware + Schnittstellenbeschreibungen
3	15.02.2012	Komplettüberarbeitung wegen neuer Geräte mit der Bestellnummernendung 02 (neue Prozessoren)

Inhaltsverzeichnis

1 Sicherheitshinweise

Zur eigenen Sicherheit und zur Sicherheit Anderer sind die aufgeführten Sicherheitshinweise zu beachten. Die Sicherheitshinweise zeigen mögliche Gefahren auf und geben Hinweise, wie Gefahrensituationen vermieden werden können.

Im vorliegenden Handbuch werden folgende Piktogramme verwendet:



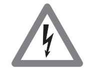
Achtung, macht auf Gefahren und Fehlerquellen aufmerksam



gibt einen Hinweis



Gefahr allgemein oder spezifisch



Gefahr eines ***Stromschlages***

1.1 Allgemein

Der REX 300 wird nur als Bestandteil eines Gesamtsystems eingesetzt.

Der Betreiber einer Maschinenanlage ist für die Einhaltung der für den speziellen Einsatzfall geltenden Sicherheits- und Unfallverhütungsvorschriften verantwortlich.

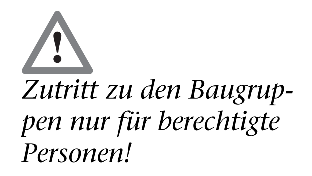
Bei der Projektierung sind die einsatzspezifischen Sicherheits- und Unfallverhütungsvorschriften zu beachten.

Not-Aus-Einrichtungen gemäß EN 60204 / IEC 204 müssen in allen Betriebsarten der Maschinenanlage wirksam bleiben. Es darf zu keinem undefinierten Wiederanlauf der Anlage kommen.

In der Maschinenanlage auftretende Fehler, die Material- oder Personenschäden verursachen können, müssen durch zusätzliche externe Einrichtungen abgefangen werden. Diese Einrichtungen müssen auch im Fehlerfall einen sicheren Betriebszustand gewährleisten. Solche Einrichtungen sind z.B. elektromechanische Sicherheitsschalter, mechanische Verriegelungen usw. (siehe EN 954-1, Risikoabschätzung).

Sicherheitsrelevante Funktionen niemals über ein Bedienterminal ausführen oder einleiten.

1.2 Zugangsbeschränkung

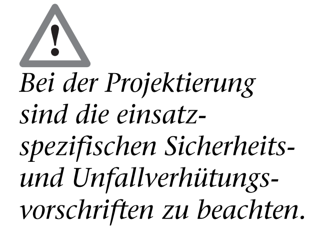


Zutritt zu den Baugruppen nur für berechtigte Personen!

Die Baugruppen sind offene Betriebsmittel und dürfen nur in elektrischen Betriebsräumen, Schränken oder Gehäusen installiert werden. Der Zugang zu den elektrischen Betriebsräumen, Schränken oder Gehäusen darf nur über Werkzeug oder Schlüssel möglich sein und nur unterwiesenem oder zugelassenem Personal gestattet werden.

1.3 Benutzerhinweise

Dieses Handbuch richtet sich an Projekteure, Anwender und Monteure die den REX 300 nutzen.



Bei der Projektierung sind die einsatzspezifischen Sicherheits- und Unfallverhütungsvorschriften zu beachten.

Dem Anwender soll die Bedienung des REX 300 aufgezeigt und die Signalisierungsfunktionen erklärt werden. Dem Monteur sollen alle zur Montage notwendigen Daten bereitgestellt werden.

Die MPI/PROFIBUS Funktion des REX 300 ist für den Gebrauch mit S7-300 sowie S7-400 Automatisierungsgeräten der Firma Siemens vorgesehen.

Der REX 300 wird ausschließlich in Verbindung mit einem Gesamtsystem eingesetzt. Aus diesem Grund sind vom Projekteur, Anwender und Monteur die für den jeweiligen Einsatzfall geltenden Normen, Sicherheits- und Unfallverhütungsvorschriften unbedingt zu beachten. Der Betreiber des Automatisierungssystems ist für die Einhaltung dieser Vorschriften verantwortlich.

1.4 Bestimmungsgemäßer Gebrauch

Der REX 300 darf nur, wie im Handbuch beschrieben, als Kommunikations- und Signalisierungssystem verwendet werden.

1.5 Bestimmungswidrigen Gebrauch vermeiden!

Unkontrollierte Wiederanläufe programmtechnisch ausschließen.

Sicherheitsrelevante Funktionen dürfen nicht über den REX 300 allein gesteuert werden. Unkontrollierte Wiederanläufe sind programmtechnisch auszuschließen.

2 Installation und Montage

Bevor Installationsarbeiten durchgeführt werden, müssen alle Systemkomponenten spannungsfrei geschaltet werden.

Die Installation und Montage muss nach VDE 0100 / IEC 364 erfolgen. Da es sich um IP20 Baugruppen handelt, müssen sie in einem Schaltschrank eingebaut werden.

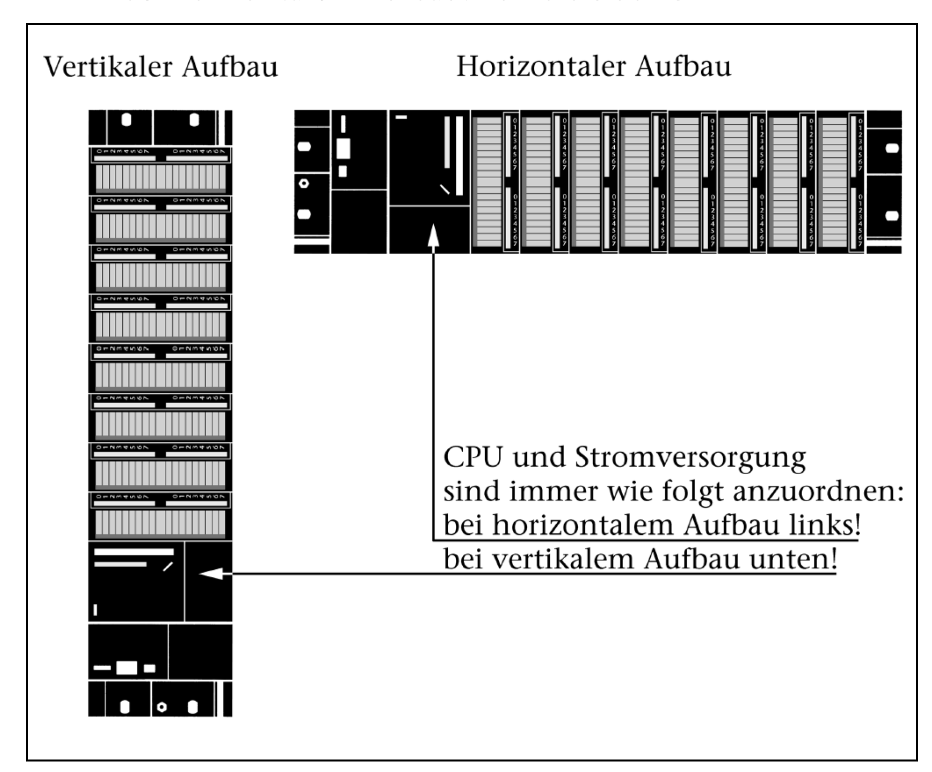
Eine Umgebungstemperatur von 0 bis 50 °C für einen sicheren Betrieb ist zu beachten.

2.1 Einbaulage

Der REX 300 kann sowohl vertikal als auch horizontal montiert werden.

Zulässige Umgebungstemperatur:

- bei vertikalem Aufbau: von 0 bis 30 °C
- bei horizontalem Aufbau: von 0 bis 50 °C



2.2 Mindestabstand

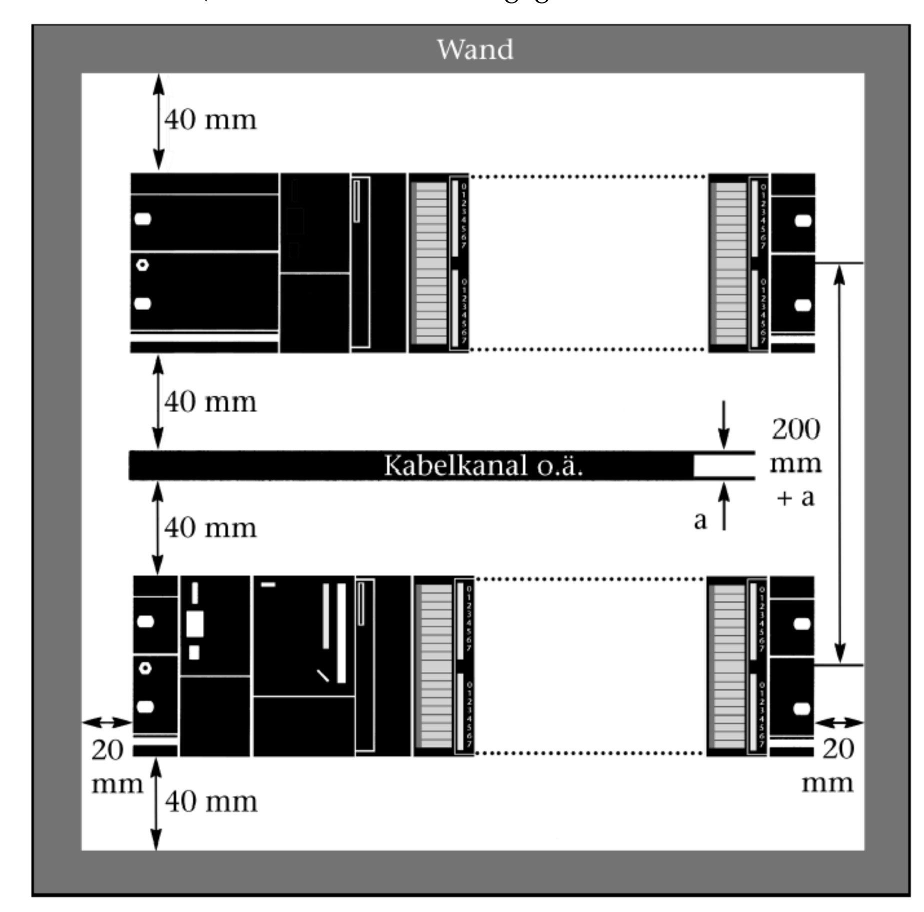
Durch die Einhaltung von Mindestabständen

- ist eine Abkühlung des REX 300 gewährleistet
- ist genügend Raum zum Ein- und Aushängen der Baugruppen vorhanden
- ist genügend Raum zum Verlegen von Leitungen vorhanden
- erhöht sich die Einbauhöhe des Baugruppenträgers auf 185 mm, wobei trotzdem das Abstandsmaß von 40 mm eingehalten werden muss

Im folgenden Bild sind für S7-300 Aufbauten auf mehreren Baugruppenträgern die Mindestabstandsmaße zwischen den jeweiligen Baugruppenträgern sowie zu benachbarten Schrankwänden, Betriebsmitteln, Kabelkanälen etc. angegeben.



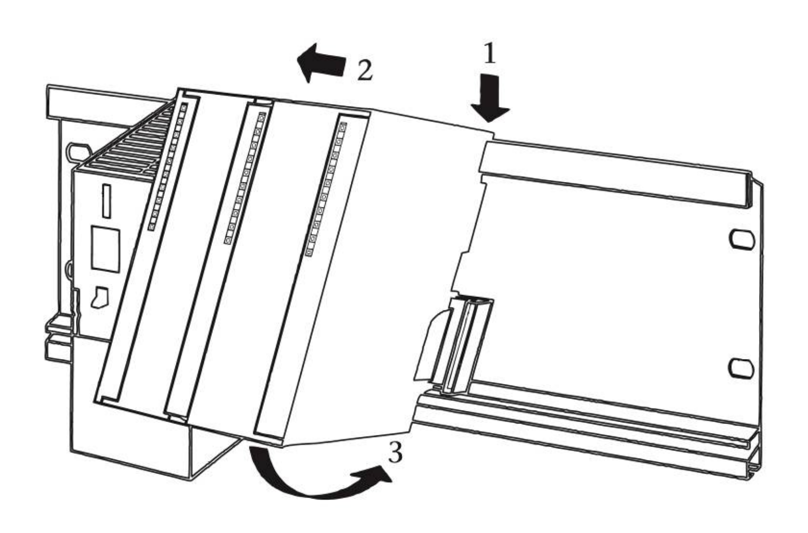
Nichteinhaltung der Mindestabstände kann die Baugruppe bei hohen Umgebungstemperaturen zerstören!



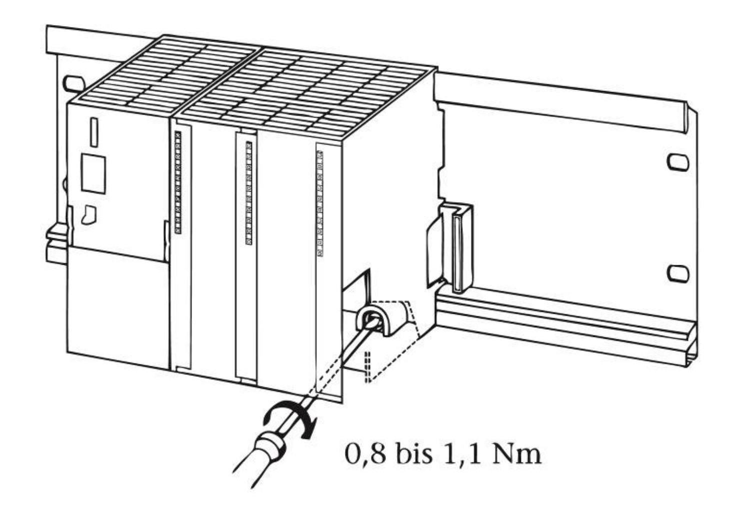
2.3 Montage der Baugruppe auf die Profilschiene

Auf die letzte Baugruppe der Zeile keinen Rückwandbusverbinder stecken. Der REX 300 ist entweder vor der CPU/Netzteil oder nach allen anderen Baugruppen anzubringen, da der Rückwandbus beim REX 300 nicht vorhanden ist und nicht durchgereicht wird.

Die Baugruppe einhängen (1), bis an die linke Baugruppe heranschieben (2) und nach unten schwenken (3).



Die Baugruppe mit einem Drehmoment von 0,8 bis 1,1 Nm fest-
schrauben.



3 Systemübersicht

3.1 Anwendung und Funktionsbeschreibung



Der REX 300 ist ein Gateway zwischen einem TCP- (LAN- oder WAN-Netz) auf der einen und einem MPI- oder PROFIBUS Netz auf der anderen Seite. Zusätzlich unterstützen die REX 300 Geräte mit WAN-Schnittstelle das RS-232, RS-485 und RS-422 Protokoll (2- und 4-Draht), für die Anbindung serieller Geräte.

Zum Nutzdatenaustausch mit dem Automatisierungssystem stehen TCP-seitig drei Protokolle zur Verfügung (Multiprotokollbetrieb):

- ein proprietäres Protokoll, welches zur Anbindung an den hauseigenen NETLink-S7-NET Treiber verwendet wird,
- das Standard TCP Protokoll und
- das von Visualisierungsherstellern oft verwendete S7-TCP/IP-Protokoll, welches auch unter dem Namen *‚RFC1006'* oder *‚ISO on top of TCP'* bekannt ist.

Es können bis zu 6 TCP- und 6 MPI-/PROFIBUS-Verbindungen gleichzeitig genutzt werden.

Sowohl TCP-, als auch feldbusseitig kann die verwendete Baudrate automatisch ermittelt werden (Auto negotiation bzw. Autobaud).

Der REX 300 wird über den beigelegten Stecker über eine externe Spannungsquelle versorgt.

Für die Verbindung des REX 300 mit dem Automatisierungssystem ist entweder eine aktive PROFIBUS Steckleitung zu verwenden oder das Gerät ist direkt in den PROFIBUS einzubinden. Durch die aktive Ausführung entstehen keine Stichleitungen, die den Bus stören könnten, wenn eine direkte Einbindung in den PROFIBUS nicht möglich ist.

Durch die Verwendung des NETLink-S7-NET Treibers ist es möglich den REX 300 PC-seitig als

- Programmieradapter,
- Fernwartungseinheit oder
- Bedien- und Beobachtungseinheit

einzusetzen.

In diesen Fällen kann der REX 300 über einen Switch, Hub, LAN Kabel oder über Internet bzw. VPN mit dem PC verbunden werden.

Mit Hilfe von myREX24.net und REX 300 Geräten mit VPN Option ist es möglich eine sehr einfache Fernwartungslösung aufzubauen. Die Verbindung wird unter Verwendung von myREX24.net jeweils vom Fernwartungspersonal und vom REX 300 zum VPN Portal myREX24.net aufgebaut. Dadurch stellen Provider- oder Kundenfirewalls kein Problem mehr dar.

3.2 Leistungsmerkmale

- Vollständige Konfiguration des Routers über Weboberfläche durch lokal angeschlossenen PC oder von der Ferne aus.
- Konfiguration laden über USB
- Weltweit einsatzfähig durch verschiedene Modem-anschaltungen (ISDN, Analog, GSM wie GPRS/EDGE/UMTS bzw. HSDPA und Zugriff über LAN und Internet
- Herstellung sicherer Verbindungen durch integrierte Fire-wall mit IP-Filter, NAT, Port-Forwarding und VPN mittels Verschlüsselungsverfahren AES, DES/3DES und Authentisie-rung mittels Pre-Shared-Key oder X.509 Zertifikate.
- Integrierter Server zum Sichern sämtlicher Einstellungen, Schlüssel und Zertifikate und zur Freigabe von Daten im Netzwerk über angeschlossenen USB-Speicher oder USB-Festplatte.
- Konfigurierbare RS-Schnittstelle RS232, RS485 und RS422
- MPI/PROFIBUS Schnittstelle zum Anschluss von S7-300 und S7-400 Systemen
- RFC1006 Protokoll zur Verwendung mit OPC-Servern oder als projektierbare Schnittstelle

3.3 Hinweise bei Verwendung von GSM-Geräten

Die Geräte mit GSM (GPRS/EDGE/UMTS) Modem unterstützen die Funkfrequenzen 850, 900, 1800, 1900 und 1900-2200(UMTS) Mhz. Wenn eine Einwahl ins Internet über GSM erfolgen soll, muss be-achtet werden, dass ein entsprechender Datentarif auf Ihrer Mobil-funkkarte (SIM) freigeschaltet ist.

3.3.1 GPRS

GPRS (General Packet Radio Service) ist ein erweiterter Dienst im GSM-Netz. Der REX 300 nutzt GPRS um Daten im GSM-Netz pa-ketorientiert zu übertragen, d. h., die Verbindung zur Gegenstelle wird nur dann belegt, wenn Daten übertragen werden. Deshalb braucht kein Funkkanal dauerhaft, wie es bei CSD der Fall ist, für einen Benutzer reserviert zu werden. GPRS-Abrechnungen sind deshalb hauptsächlich von den übertragenen Datenmengen ab-hängig und nicht von der Verbindungsdauer.

Die REX 300 Reihe arbeitet mit einer Geschwindigkeit von ca. 55 - 85 kBit/s, wenn GPRS verfügbar ist. Des Weiteren wird der Sprach-ruf dem Datenruf vorgezogen wodurch die Bandbreite des Daten-rufs zugunsten der Qualität des Sprachanrufs geschmälert wird. Be-legen mehrere Sprachanrufe eine Funkzelle, dann verbleibt ein ge-ringer Datendurchsatz für die GPRS-Verbindung.

3.3.2 EDGE

Mit dem Enhanced Data Rates for GSM Evolution erhöht sich der Datendurchsatz. Bei EDGE wird eine Datenübertragungsrate von bis zu 59,2 kBit/s pro Zelle ermöglicht. Bei Verwendung von acht Zellen werden bis zu 473 kBit/s erreicht. Im Vergleich hierzu sind mit dem Datendienst GPRS theoretisch maximal 171,2 kBit/s möglich. Der Wechsel des Modulationsverfahrens geschieht selektiv nur auf den Kanälen, die von EDGE-fähigen Geräten belegt werden. Dadurch ist eine gleichzeitige störungsfreie Nutzung von GSM/GPRS- und EDGE-fähigen Endgeräten in derselben Funkzelle möglich.

Die derzeit marktüblichen Endgeräte, wie auch der REX 300, sind solche der EDGE-Klasse 10. Dies bedeutet, dass diese Geräte über maximal vier Downlinkslots sowie zwei Uplinkslots verfügen. Hieraus resultiert eine mögliche Datenübertragungsrate von effektiv ca. 150 - 240 kBit/s im Down- und 110 kBit/s im Upload.

3.3.3 UMTS

UMTS ist ein Mobilfunkstandard der dritten Generation (3G). Mit diesem sind deutlich höhere Datenraten, als z. B. mit EDGE, möglich. Der REX 300 unterstützt UMTS als auch den darauf aufbauenden HSDPA/HSUPA Dienst.

3.4 Lieferumfang

Bitte prüfen Sie, ob alle aufgeführten Artikel in der Produktpackung enthalten sind.

- Router REX 300



- Netzwerkkabel gekreuzt (Crossover) (3m)



- Bei den Routervarianten mit Analogmodem:
  1x Kabel mit RJ11-Steckern (4P2C) und 1x Kabel mit TAE-Stecker



- Bei den Routervarianten mit ISDN-Modem:
  1x Kabel mit RJ11-Steckern (4P4C)



- Quickstart Guide



- Produkt-CD (REX 300)



Sollte einer dieser aufgeführten Artikel fehlen, wenden Sie sich bitte an folgende Adresse:

Systeme Helmholz GmbH

Hannberger Weg 2

D-91091 Großenseebach

Tel.: +49 9135 7380-0

Fax.: +49 9135 7380-110

E-Mail: info@helmholz.de

Internet: www.helmholz.de

3.5 Zubehör

Für den REX 300 sind folgende Zubehörteile zusätzlich erwerbbar.

- RS232 Adapterkabel 3m (REX 300 mit WAN Anschluss, außgenommen REX 300 eco Geräte der Bestellnummer 700-874-xxxxx))

  Bestellnummer: 700-879-1VK11

- S7-200 Adapterkabel 3m (REX 300 mit WAN Anschluss, außgenommen REX 300 eco Geräte der Bestellnummer 700-874-xxxxx))

  Bestellnummer: 700-879-1VK21

- Profilschienenadapter für Hutschiene

  Bestellnummer: 700-390-6BA00

4 Anzeige und Bedienelemente

4.1 Ansicht Geräteoberseite



Pos.	Bezeichnung	Status	Beschreibung
1	SF	LED aus	Router arbeitet fehlerfrei
		LED ein	Ein Fehler ist aufgetreten. Diagnose unter Status > System
2	Con VPN	LED aus	Keine Internetverbindung aktiv
		LED ein	Internetverbindung aktiv
		LED blinkt	VPN-Verbindung aktiv
		LED blinkt schnell	Router versucht Internet oder VPN-Verbindung aufzubauen
3	RxD	LED aus	Keine Buskommunikation
		LED ein	Buskommunikation OK (Blinkt auch beim Start des Gerätes und gleichzeitigem laden einer Konfigurationsdatei von einem USB-Speicher)
4	TxD	LED aus	Kein Datentransfer an MPI
		LED blinkt	Datentransfer an MPI
5	Rdy	LED ein	Nach dem Einschalten ist die Ready-LED für ca. 10 Sekunden aus, während die Power-LED sofort leuchtet. Nach ca. 10 Sekunden blinkt die Ready-LED. Nach ca. 110 Sekunden sollte die Ready-LED dauerhaft leuchtet.
		LED blinkt	

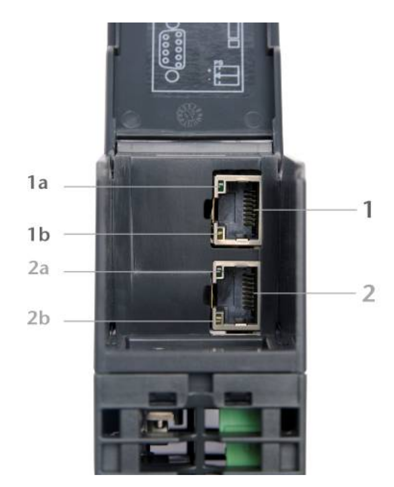
6	ON	LED aus	Stromversorgung nicht angeschlossen oder ausgeschaltet
		LED ein	Stromversorgung angeschlossen und eingeschaltet
7	FME (nur GSM)	-	Antennenanschluss für GSM-Antennen

4.2 Ansicht Geräteunterseite



Pos.	Bezeichnung	Beschreibung
1	PE-Bleche	Für die PE-Verbindung zur Profilschiene
2	Schraube	Zur Montage auf der Profilschiene

4.3 Ansicht Netzwerkschnittstellen



Pos.	Bezeichnung	Status	Beschreibung
1	WAN	-	WAN-Anschluss des Routers
1a	WAN-LED	grün	Netzwerkverbindung vorhanden
1b	WAN-LED	orange	Netzwerkdatenverkehr aktiv
2	LAN	-	Anschluss des lokalen Netzwerkes
2a	LAN-LED	grün	Netzwerkverbindung vorhanden
2b	LAN-LED	orange	Netzwerkdatenverkehr aktiv

4.4 Ansicht Kommunikationsschnittstelle (GSM)



Pos.	Bezeichnung	Beschreibung
1	USB	USB Schnittstelle für den Anschluss eines USB Datenspeichers wie z.B. einem USB-Stick.
2	Dial out	Taste zum Aufbau einer Internet- oder VPN-Verbindung und Zurücksetzen auf Werkseinstellungen.
3	PROFIBUS	MPI/PROFIBUS Schnittstelle zur Anbindung von Geräten mit MPI oder PROFIBUS Schnittstelle bis 12 MBit/s
4	SIM	SIM-Kartenslot für die SIM-Karte. Diese wird direkt in den Slot gesteckt. Für eine bildliche Beschreibung des Einlegeverfahrens sehen Sie bitte im Kapitel XXXXX nach.
5	PS	Anschlussstecker für die Spannungsversorgung

4.5 Ansicht Kommunikationsschnittstelle (ISDN/Analog)



Pos.	Bezeichnung	Beschreibung
1	USB	USB Schnittstelle für den Anschluss eines USB Datenspeichers wie z.B. einem USB-Stick.
2	Dial out	Taste zum Aufbau einer Internet- oder VPN-Verbindung
3	PROFIBUS	MPI/PROFIBUS Schnittstelle zur Anbindung von Geräten mit MPI oder PROFIBUS Schnittstelle bis 12 MBit/s
4	TAE	RJ-12 Buchse zum Anschluss des im Router integrierten Analog- bzw. ISDN-Modems
5	PS	Anschlussstecker für die Spannungsversorgung

4.6 Ansicht Kommunikationsschnittstelle (eco-Geräte)

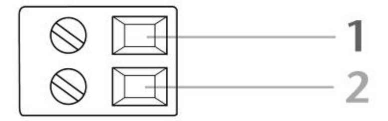


Pos.	Bezeichnung	Beschreibung
1	USB	USB Schnittstelle für den Anschluss eines USB Datenspeichers wie z.B. einem USB-Stick.
2	Dial out	Taste zum Aufbau einer Internet- oder VPN-Verbindung
5	PS	Anschlussstecker für die Spannungsversorgung

5 Schnittstellen

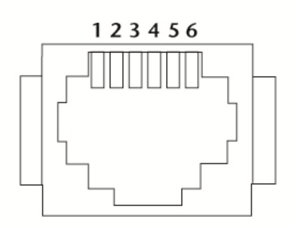
5.1 Belegung

5.1.1 Anschlussbelegung Versorgungsspannung



Pos.	Bezeichnung	Beschreibung
1	+	Anschluss Versorgungsspannung 10-30 VDC
1a	-	Anschluss 0 V DC

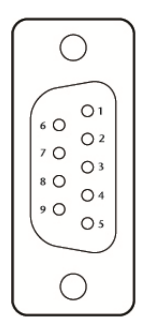
5.1.2 Anschlussbelegung der RJ12 Buchse



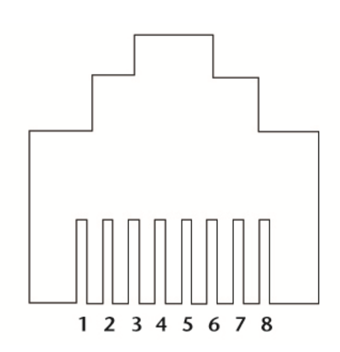
Pos.	ISDN	Analog
1	Nicht belegt	Nicht belegt
2	TX+	Nicht belegt
3	RX+	Lb/b
4	RX-	La/a
5	TX-	Nicht belegt
6	Nicht belegt	Nicht belegt

5.1.3 Anschlussbelegung der MPI/PROFIBUS Schnittstelle

Pos.	MPI/PROFIBUS
1	Nicht belegt
2	GND 24 V
3	Datenleitung B
4	Sendeanforderung
5	GND 5 V (200 mA)
6	5 V Ausgang
7	24 V Versorgungseingang
8	Datenleitung A
9	Sendeanforderung

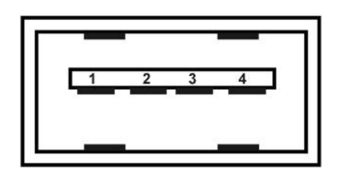


5.1.4 Belegung der RJ45 Buchse für serielles Kabel



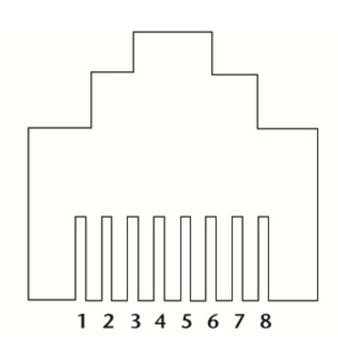
Pos.	RJ45 Buchse RS232	RJ45 Buchse RS485
1	CTS (Clear to Send)	RxD + (Receive Data)
2	RTS (Request to Send)	TxD – (Transmit Data)
3	DSR (Data Set Ready)	Nicht belegt
4	Signal Ground	Signal Ground
5	DTR (Data Terminal Ready)	+5 Volt (nur bei 4-Draht-Betrieb)
6	TxD (Transmit Data)	TxD + (Transmit Data)
7	RxD (Receiver Data)	RxD – (Receive Data)
8	DCD (Data Carrier Detect)	Nicht belegt

5.1.5 Belegung des USB-Anschlusses an der Frontseite



Pos.	USB
1	VCC (+5V)
2	- Data
3	+ Data
4	GND

5.1.6 Belegung der LAN- bzw. WAN-Schnittstelle



Pos.	LAN/WAN
1	TX+
2	TX-
3	RX+
4	Nicht belegt
5	Nicht belegt
6	RX-
7	Nicht belegt
8	Nicht belegt

6 Inbetriebnahme des Routers

Wenn der Router auf einer Hutschiene montiert werden soll, dann kann dafür ein separat erhältlicher Adapter verwendet werden.

Bestellnummer: 700-390-6BA00



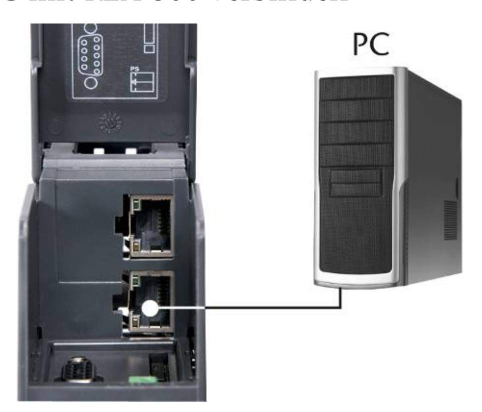
Bitte auf richtige Polung und Kontakt der PE-Belche zu einem Potentialausgleich achten!

Der Router ist für den Schaltschrankeinbau vorgesehen. Das Gerät ist konzipiert für die Montage auf einer Profilschiene. Der Potentialausgleich des Gerätes wird über die PE-Bleche an der Unterseite des Gerätes durchgeführt. Die nun durchgeführten Schritte sind im beiliegenden Quickstart Guide näher beschrieben.

1. Versorgungsspannung anschließen

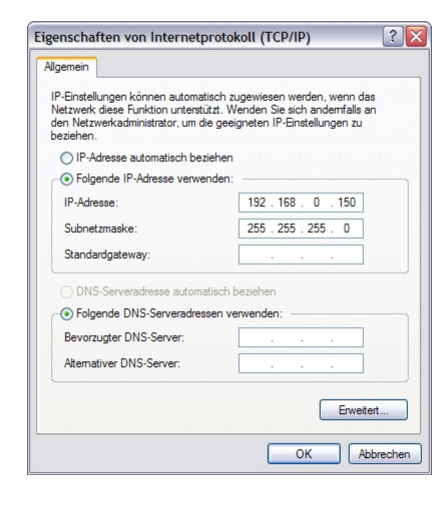


2. PC mit REX 300 verbinden

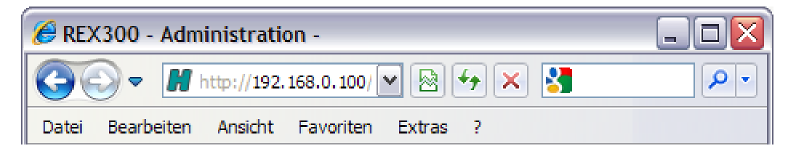


3. IP-Adresse des PCs an die IP-Adresse des REX 300 anpassen

In den Einstellungen Ihrer Netzwerkkarte muss eine feste IP-Adresse aus dem Bereich 192.168.0.1 bis 192.168.0.254 eingestellt sein. Bitte verwenden Sie nicht die IP-Adresse 192.168.0.100, da dies die Default IP-Adresse des REX 300 ist.



4. Starten Sie Ihren Browser und geben Sie in der Adresszeile die erforderliche IP-Adresse des Routers ein. Die IP-Adresse des Routers bei Auslieferung lautet: 192.168.0.100



5. Nun müssen Sie sich mit folgenden Einstellungen am Router anmelden:

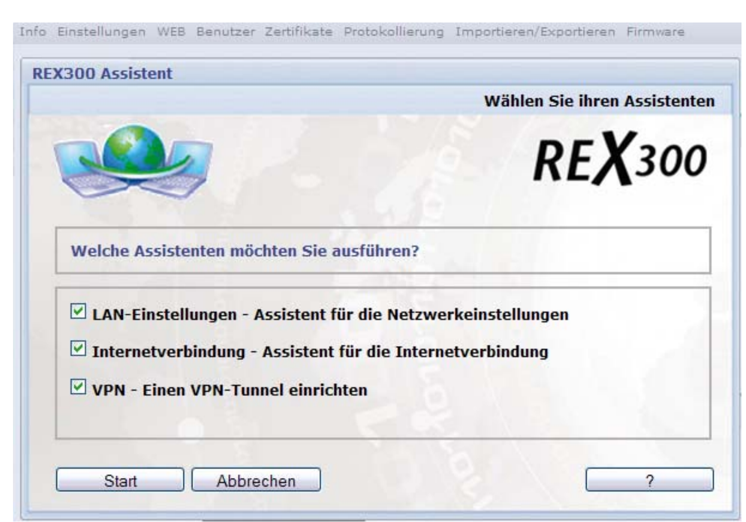
   Benutzername: helmholz
   Kennwort: router



6. Nach erfolgreicher Anmeldung wird Ihnen die Startseite des REX 300 Webinterface angezeigt. Für eine manuelle Konfiguration können Sie entweder alle Parameter selbst einstellen oder die Assistenten über den Link in der rechten oberen Ecke starten.
   Hier können Sie Assistenten für Netzwerk-, Internet- und VPN-Einstellungen ausführen. Der Assistent leitet Sie Schritt für Schritt durch die Konfigurationsprozesse und funktioniert intuitiv. Sie können den Assistenten auch manuell aufrufen.

!

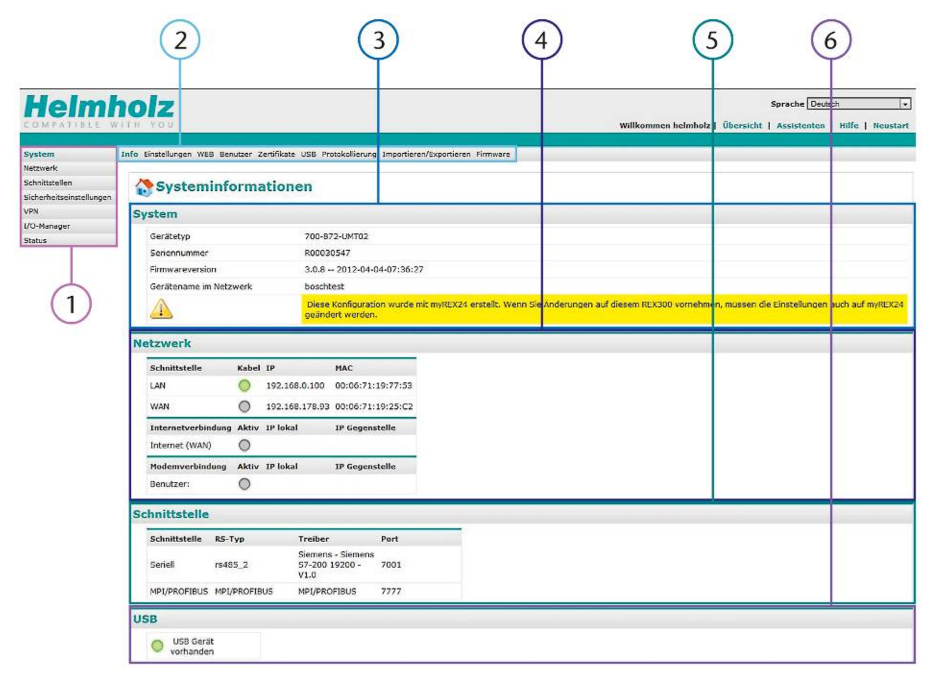
Die Einstellungen, die der Assistent für Sie automatisch vornimmt, können ebenfalls per Hand in den einzelnen Menüpunkten eingestellt werden.



7 Grundkonfiguration des Routers über die Weboberfläche

7.1 Die Startseite der Weboberfläche

Die Startseite ist so konzipiert, dass Sie auf einen Blick die wichtigsten Informationen über den Zustand bzw. Zugriff auf den Router REX 300 erhalten. Die seitliche Navigationsleiste (1) und die obere Navigationsleiste (2) werden Sie während der Konfiguration des Routers begleiten. Zu jedem der in der seitlichen Navigationsleiste (1) aufgeführten Punkte werden entsprechende Unterpunkte (2) in der oberen Navigationsleiste angezeigt.



Pos.	Bezeichnung	Funktion/Beschreibung
1	Seitliche Navigationsleiste	Diese Navigationsleiste kann als Hauptmenü angesehen werden.
2	Obere Navigationsleiste	Diese Navigationsleiste bietet die Unterpunkte zu entsprechend ausgewähltem Hauptmenü.
3	System	Systeminformationen wie Gerätetyp, Gerätename, aktueller Firmwarestand und Seriennummer des Routers.

4	Netzwerk	**Interface: LAN-WAN:** Zeigt an, welche Netzwerkanschlüsse im Augenblick im bestehenden Netzwerk über die entsprechenden Buchsen verbunden / angeschlossen sind. Eine bestehende Verbindung wird durch ein grünes Symbol angezeigt. **Internetverbindung:** Eine momentan aktive Verbindung ins Internet wird durch einen grün ausgefüllten Kreis dargestellt. Besteht dagegen momentan keine aktive Verbindung ins Internet, dann wird dies durch einen grau ausgefüllten Kreis angezeigt. **Modem Verbindung:** Hier werden nur die eingehenden Modemverbindungen angezeigt. Falls eine Verbindung mit dem Modem hergestellt wurde, wird dies durch einen grün ausgefüllten Kreis dargestellt. Zugleich wird der Benutzer angezeigt, der mit dem Modem verbunden ist.
5	Schnittstelle	Hier wird die aktuelle Konfiguration der Seriell und MPI/PROFIBUS Schnittstelle angezeigt.
6	USB	Information über angeschlossenen USB-Speicher. Ein angeschlossener Speicher (z.B. USB-Stick oder extern angeschlossene Festplatte) wird durch einen grün ausgefüllten Kreis dargestellt.

7.2 Beschreibung der Symbole, Schaltflächen und Felder

Im weiteren Verlauf dieser Bedienungsanleitung werden Sie immer wieder auf bestimmte Symbole stoßen, deren Bedeutung auf der folgenden Seite ausführlich beschrieben werden.

Symbol oder Feldertypen	**Funktion/Beschreibung**
	Grau dargestellte LED: Verbindung nicht aktiv/Kabel nicht angeschlossen. Grün dargestellte LED: Verbindung aktiv bzw. Kabel angeschlossen.
Änderungen temporär speichern	Diese Schaltfläche erscheint immer dort, wo Einstellungen vorgenommen werden können. Sie dient zum temporären Abspeichern der momentanen Konfiguration, d. h. wird der Router neu gestartet, dann sind die geänderten Einstellungen verloren. Zum dauerhaften Abspeichern der Einstellungen ist die Schaltfläche *„Änderungen übernehmen“* anzuklicken.
Änderungen löschen	Wenn Sie Ihre Eingaben zuvor nur temporär gespeichert haben *„Änderungen speichern“*, dann können Sie diese hiermit durch Betätigen dieser Schaltfläche zurücksetzen.
Änderungen übernehmen	Hiermit werden alle gespeicherten Änderungen dauerhaft auf dem Router gespeichert und übernommen.
	Sog. Checkbox. Durch Anklicken des entsprechenden Feldes kann die jeweilige Option aktiviert/deaktiviert werden.
	In diesem Eingabefeld müssen Sie, falls erforderlich, die Eingabe per Hand durchführen.
	Durch Betätigen des mit einem Pfeil markierten Kästchens treffen Sie bitte die entsprechende Auswahl (Auswahlfeld).
	Wenn Sie dieses Feld betätigen, dann können Sie die Einstellungen in der entsprechenden Zeile ändern (editieren).
	Um die in der entsprechenden Zeile durchgeführten Änderungen rückgängig zu machen, klicken Sie bitte auf diese Schaltfläche.

	Hiermit speichern Sie temporär die momentan bearbeiteten Einstellungen. Um die Änderungen im Router dauerhaft abzuspeichern, ist die Schaltfläche *„Änderungen übernehmen“* zu betätigen.
	Mit diesem Feld können Sie Zeilen für weitere Eingaben hinzufügen. Bevor Sie dieses Feld betätigen, muss die momentan angezeigte Zeile Werte bzw. Angaben enthalten. Ansonsten erfolgt eine Fehlermeldung im oberen Bereich der aktuellen Konfigurationsseite.
	Hiermit löschen Sie die entsprechenden Eingaben in der momentanen Bearbeitungszeile.
	Hiermit können Sie die Reihenfolge von Regeln ändern.

7.3 System – Einstellungen

Bevor Sie den Industrierouter REX 300 speziell für Ihren Anwendungsfall konfigurieren, sollten Sie vorab bestimmte Grundeinstellungen vornehmen. Gehen Sie hierzu wie nachfolgend beschrieben vor:

- Klicken Sie auf der Startseite der Weboberfläche in der oberen Navigationsleiste auf die Schaltfläche **System** und **Einstellungen**. Es wird daraufhin die nachfolgende Menümaske mit den Systemeinstellungen angezeigt. Gehen Sie nun, wie auf den folgenden Seiten beschrieben, entsprechend vor.



<table>
<tr><th>Bezeichnung</th><th>Funktion/Beschreibung</th></tr>
<tr><td>Gerätename im Netzwerk</td><td>Vergeben Sie einen Namen für den Router.</td></tr>
<tr><td>Gerätebeschreibung</td><td>Um den Router in einem Netzwerk zu identifizieren, geben Sie hier eine sinnvolle Beschreibung ein.</td></tr>
<tr><td>System Neustart …[h]</td><td>Um den Router in bestimmten Abständen neu zu starten, tragen Sie hier die Anzahl der gewünschten Stunden ein.</td></tr>
<tr><td>Datum/Uhrzeit (UTC)</td><td>Anzeige der aktuellen Systemzeit in Universal Time Coordinates (UTC).</td></tr>
<tr><td>Datum/Uhrzeit lokal</td><td>Anzeige der Uhrzeit anhand der Einstellungen der Zeitzone.</td></tr>
<tr><td>Einstellen Datum/Uhrzeit lokal</td><td>Geben Sie hier die Zeit ein, falls kein NTP-Server eingestellt ist bzw. wenn der NTP-Server nicht erreichbar ist.
Beispiel: 2010.03.31-14:30:00
<table>
<tr><th>Format</th><th>Bedeutung</th></tr>
<tr><td>JJJJ</td><td>Jahr z. B. 2010</td></tr>
<tr><td>MM</td><td>Monat z. B. 03</td></tr>
<tr><td>TT</td><td>Tag z. B. 31</td></tr>
<tr><td>HH</td><td>Stunde z. B. 14</td></tr>
<tr><td>MM</td><td>Minute z. B. 30</td></tr>
<tr><td>SS</td><td>Sekunden z. B. 00</td></tr>
</table></td></tr>
<tr><td>Zeitzone</td><td>Klicken Sie auf das Auswahlfeld und wählen Sie die Zeitzone aus, in der Sie sich befinden. Eingestellte Zeitzone: Berlin, Germany</td></tr>
<tr><td>NTP-Server</td><td>Wird die Checkbox durch Anklicken mit einem Haken versehen, dann bezieht der Router seine Zeit von einem anderen Rechner (falls in nachfolgender Eingabebox eingetragen) und zeigt die aktuelle Systemzeit an. Die Uhrzeit wird alle zwei Stunden per NTP aktualisiert. Eingetragener Zeitserver: 0.de.pool.ntp.org</td></tr>
<tr><td>NTP-Server</td><td>Eingabe eines Zeitservers zum Erhalt der aktuellen Systemzeit. Statt des DNS-Namens kann auch die IP-Adresse des Zeitservers eingetragen werden. Bei Eingabe eines DNS-Namens muss ein DNS-Server in den Netzwerkeinstellungen eintragen sein.</td></tr>
</table>

Maileinstellungen	Wird die Option *„automatische Maileinstellungen aktivieren“* = *„Ja“* verwendet, so benutzt der Router den Mailserver der Systeme Helmholz GmbH.
SMTP-Server	Der SMTP-Server wird benötigt, damit der Router E-Mails versenden kann.
SMTP-Port	Eingabe des Ports, über den die E-Mails versendet werden. In der Regel handelt es sich hierbei um den Port 25.
E-Mail-Adresse	Tragen Sie hier die Absenderadresse des gewünschten E-Mail-Absenderkontos ein.
SMTP benötigt Authentifizierung	Abhängig vom Provider ist die Checkbox abzuhaken oder nicht. Erfragen Sie die entsprechende Einstellung bei Ihrem Provider oder Administrator.
Benutzer Passwort	Zur Authentifizierung am SMTP-Server werden Benutzer und Passwort benötigt. D. h. will der Router eine E-Mail an den SMTP senden, dann muss sich der Router gegebenenfalls authentifizieren.

7.4 Sicherheitseinstellungen

Um von außen auf die Weboberfläche des Industrierouters zu gelangen, ist die interne Firewall des Routers so zu konfigurieren, dass der Port 80 für eingehende Anfragen freigegeben ist.

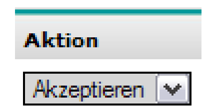
1. Wechseln Sie auf die Seite „**Sicherheitseinstellungen**“ – **WAN>LAN**.



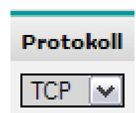
2. Klicken Sie auf die Checkbox um diese mit einem Haken zu versehen.



3. Wählen Sie über das Auswahlfeld die Option *„Akzeptieren“* aus.



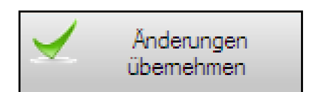
4. Wählen Sie unter Protokoll über die Auswahlfläche die Einstellung *„TCP“* aus.



5. Tragen Sie unter Ziel-Port die Zahl *„80“* ein.
6. Danach speichern Sie ihre Eingaben mit der Schaltfläche *„Zeile hinzufügen“*.



7. Zum dauerhaften Abspeichern klicken Sie auf *„Änderungen übernehmen“*.



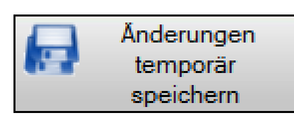
7.5 Einstellungen sichern

Wenn Sie die vorher beschriebenen Systemeinstellungen abgeschlossen haben, sichern Sie diese zunächst temporär durch Anklicken der Schaltfläche *„Änderungen speichern“*.

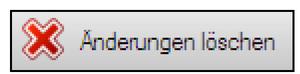
!

Bitte beachten Sie!

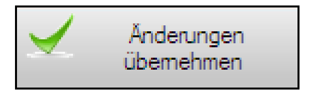
Damit Ihre durchgeführten Einstellungen dauerhaft gespeichert sind und z. B. nach dem Neustart oder Ausschalten des Routers noch vorhanden sind, müssen Sie grundsätzlich wie hier beschrieben vorgehen, da ansonsten die Einstellungen nach einem Neustart des Routers verloren gehen.



Falls Sie Ihre Eingaben nochmals auf die ursprüngliche Einstellung zurücksetzen wollen, dann betätigen Sie die Schaltfläche *„Änderungen löschen“*.



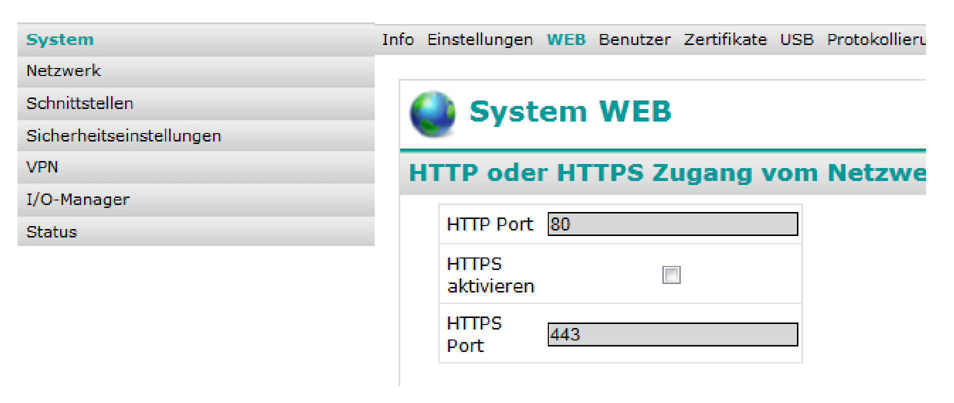
Zur dauerhaften Speicherung der Einstellungen auf dem Industrierouter REX 300 klicken Sie jetzt auf die Schaltfläche *„Änderungen übernehmen“*.



Sollten bestimmte Eingaben fehlen oder fehlerhaft sein, dann werden die entsprechenden Fehlermeldungen im oberen Bereich der Konfigurationsseite angezeigt. Überprüfen Sie daraufhin nochmals Ihre Einstellungen.

7.6 System – WEB

Bei der Verwendung von HTTPS (Hypertext Transfer Protocol Secure) wird die Verbindung zwischen Webbrowser und Webserver verschlüsselt übertragen. Je nach Schlüssellänge meistens 40 oder 128 Bit.



Bezeichnung	Funktion/Beschreibung
HTTP Port	Der Standardport für HTTP-Anfragen ist 80 (TCP). Sollten Sie diesen Port jedoch für Ihre OpenVPN Verbindung benötigen, oder wenn dieser schon anderweitig verwendet wird, können Sie diesen Port hier ändern.
HTTPS aktivieren	Durch Auswahl der Checkbox kann das sichere Hypertext Transfer Protocol Secure aktiviert werden.
HTTPS Port	Für den Zugriff sind vom entfernten Rechner die IP-Adresse des Routers und der Port einzugeben. Hier Port 443 z. B. https://217.6.86.44:443

7.7 System – Benutzer

7.7.1 Allgemeines

Über das Benutzermanagement können Sie:

- Benutzern Zugriff auf die Administration per Weboberfläche, Modemeinwahl oder VPN-Einwahl erlauben.
- Vorhandene Benutzer editieren, löschen oder neue Benutzer anlegen

7.7.2 Benutzer editieren

Zum Editieren eines Benutzers gehen Sie bitte folgendermaßen vor:

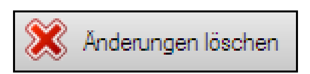
1. Wählen Sie „**System**" und dann „**Benutzer**"
2. Betätigen Sie den „*Button*" (siehe Abb.), um einen Benutzer, dessen Rechte Sie ändern möchten, zu editieren.
   Der Benutzer wird zusammen mit den Zugangseinstellungen in der ersten Zeile angezeigt.



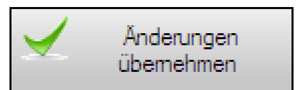
3. Wechseln Sie in die entsprechenden Eingabefelder und führen Sie die gewünschten Änderungen durch.
4. Speichern Sie Ihre Änderung mit einem Mausklick auf „*Speichern*" (siehe Abb.)



5. Sie können Ihre letzte Änderung über die Schaltfläche „*Änderungen löschen*" zurücksetzen.



6. Über die Schaltfläche „*Änderungen übernehmen*", werden die Änderungen auf den Industrierouter übertragen.



7.7.3 Benutzer anlegen

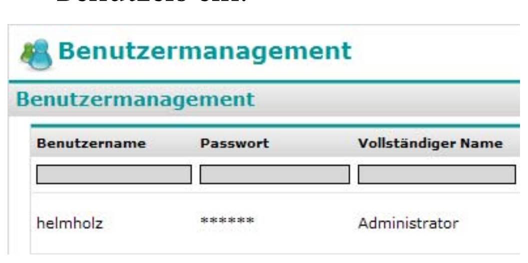



Bitte beachten Sie!

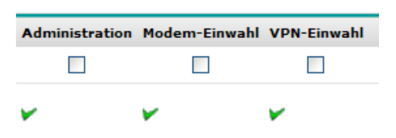
Es müssen immer alle drei Eingabefelder ausgefüllt werden, ansonsten wird beim Speichern eine Fehlermeldung ausgegeben.

Zum Anlegen eines Benutzers gehen Sie bitte folgendermaßen vor:

1. Wählen Sie in der linken Navigationsleiste „**System**“ und dann in der oberen Navigationsleiste „**Benutzer**“ aus.
2. Tragen Sie in die Eingabefelder der ersten Zeile den Benutzernamen, das Passwort und den vollständigen Namen des Benutzers ein.



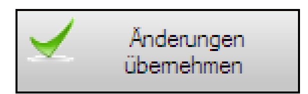
3. Legen Sie über die drei folgenden Auswahlboxen fest, welche Rechte der neue Benutzer erhalten soll. Möglich sind folgende Einstellungen:
   - Konfiguration ändern (Administration)
   - Verbindung zum internen Modem aufbauen (Modemeinwahl)
   - Eingehende VPN-Verbindung aufbauen (VPN-Einwahl)



4. Zutreffendes ist durch Anklicken der entsprechenden Auswahlbox mit einem Haken zu versehen.
5. Klicken Sie zum temporären Speichern nun auf die Schaltfläche *„Zeile hinzufügen“*.



6. Zum Übertragen der Einstellungen auf den Industrierouter betätigen Sie den Button *„Änderungen übernehmen“*.



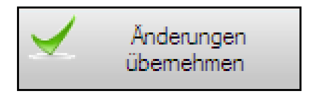
7.7.4 Benutzer löschen

Zum Löschen eines Benutzers gehen Sie bitte folgendermaßen vor:

1. Wählen Sie in der linken Navigationsleiste „**System**“ und dann „**Benutzer**“ aus.
2. Wählen Sie die Zeile aus, in der der Benutzer mit Passwort usw. aufgeführt ist, und klicken Sie auf das Symbol *„Löschen“*



3. Zum dauerhaften Speichern der Einstellungen auf den Industrierouter betätigen Sie die Schaltfläche *„Änderungen übernehmen“*.



Sie können sich nun nicht mehr mit diesem Benutzer an der Weboberfläche, der Modem- oder VPN-Einwahl anmelden bzw. authentifizieren.

7.8 System – Zertifikate

Hauptbestandteil bei VPN-Verbindungen mit IPSec bzw. OpenVPN sind die Vertrauensstellungen zwischen zwei oder mehreren Kommunikationspartnern. Die Authentifizierung wird bei der IPSec oder OpenVPN Konfiguration im Kapitel VPN eingestellt.
Für eine sichere Kommunikation ist die Prüfung der Authentizität erforderlich. Mit Hilfe von Zertifikaten wird sichergestellt, dass auch die richtigen Partner miteinander kommunizieren. Mit einem Zertifikat weist sich der Zertifikatsinhaber aus. Das Zertifikat kann von einer übergeordneten Stelle (sog. Certificate Authority kurz CA) oder vom Zertifikatsinhaber selbst ausgestellt werden. Der Zertifikatsinhaber wird dabei Subject und der Zertifikatsaussteller mit Issuer bezeichnet.
Nachfolgend sehen Sie die Bildschirmmaske mit den Registern der entsprechenden Zertifikate und deren Möglichkeit neue Zertifikate zu importieren.

7.8.1 Eigene Zertifikate

Eigene Zertifikate werden vom Zertifikatsinhaber selbst ausgestellt. Damit der Router das eigene Zertifikat bei einer Gegenstelle verwenden kann, um es dort vorzuzeigen, ist die entsprechende PKCS12-Datei (Zertifikat inklusive privatem Schlüssel) auszuwählen, um diese dann zu importieren. Es können dabei eine oder mehrere PKCS12-Dateien importiert werden. Zum eigenen Zertifikat gehört auch immer ein Schlüssel. Daher muss hier eine PKCS12-Datei importiert werden. Diese besteht nämlich aus einer .crt-Datei und einer .pem-Schlüsseldatei.

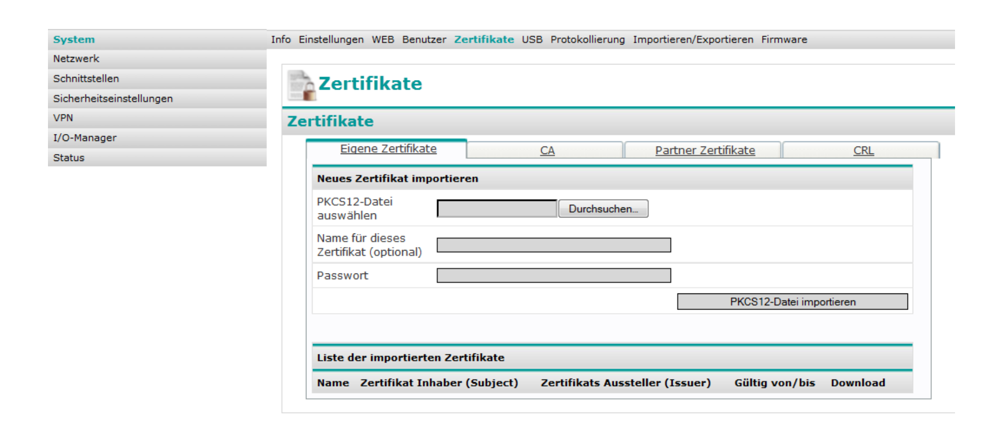
!

Bitte beachten Sie!

XCA fasst den Schlüssel und das Zertifikat zu einer Datei zusammen, deren Dateiendung „.p12“ ist. Hiermit ist jedoch die PKCS12-Datei gemeint.

Die Software XCA ist ein Programm mit einer grafischen Oberfläche zum Erstellen von Zertifikaten und kann unter der Adresse:

http://xca.sourceforge.net/ heruntergeladen werden



<table>
<tr><th>Bezeichnung</th><th colspan="2">Funktion/Beschreibung</th></tr>
<tr><td>Neues Zertifikat im-
portieren</td><td colspan="2">PKCS12-Datei auswählen:
Auswahl der Zertifikatsdatei (PKCS12-Datei).

Name für dieses Zertifikat (optional):
Optionale Eingabe des Namens für die Zertifikatsdatei.

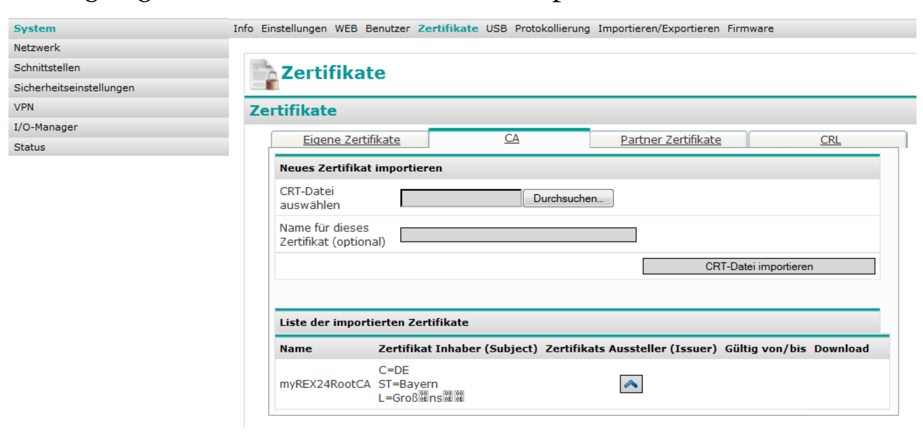
Passwort:
Eingabe des Zertifikatspasswortes. Beim Erstellen des Zertifikates muss ein Passwort vergeben worden sein, andernfalls wird das Importieren nicht zugelassen!

PKCS12-Datei importieren:
Falls die obigen Einstellungen korrekt eingegeben wurden, kann die Zertifikatsdatei durch einen Mausklick auf diesen Button importiert werden.</td></tr>
<tr><td>Liste der importierten Zertifikate</td><td colspan="2">Hier werden die bereits importierten Zertifikate aufgelistet. Weitere Zertifikatsdateien können über „PKCS12-Datei importieren“ aufgenommen werden.</td></tr>
<tr><td>Name</td><td colspan="2">Name für das Zertifikat.</td></tr>
<tr><td rowspan="8">Zertifikat Inhaber (Subject)</td><td colspan="2">Merkmale des Zertifikatinhabers</td></tr>
<tr><td>C</td><td>Ländercode z. B. DE</td></tr>
<tr><td>ST</td><td>Bundesland z. B. Bayern</td></tr>
<tr><td>L</td><td>Ort z. B. Großenseebach</td></tr>
<tr><td>O</td><td>Firma z. B. Systeme Helmholz</td></tr>
<tr><td>OU</td><td>Firmenabteilung z. B. Support</td></tr>
<tr><td>CN</td><td>Üblicher Name z. B. Zertifikate</td></tr>
<tr><td>E</td><td>E-Mail-Adresse z. B. mustermann@muster.de</td></tr>
<tr><td>Zertifikats Aussteller</td><td colspan="2">Beschreibung siehe vorher (Zertifikat Inhaber – Subject)</td></tr>
<tr><td>Gültig von / bis</td><td colspan="2">Anzeige des Zeitraumes, während dem das Zertifikat Gültigkeit besitzt.</td></tr>
</table>

Download		Nach Betätigen dieses Buttons erscheint ein weiterer Bereich. Zum Download ist mit der rechten Maustaste auf den Link zu klicken und die Option *„Ziel speichern unter …“* auszuwählen.
		Nach Betätigen dieses Buttons kann die Liste der importierten Zertifikate zurückgesetzt bzw. gelöscht werden.

7.8.2 CA

Durch ein Stammzertifikat wird überprüft, ob das Zertifikat von der Gegenstelle auch vom Stammzertifikat signiert wurde. Ein solches Stammzertifikat muss dann importiert werden, wenn unter den VPN-Einstellungen als Authentisierungsmethode *„durch ein Zertifikat von derselben CA"* gewählt wird. Als Entscheidungskriterium, ob das Zertifikat des sich Einwählenden gültig ist, wird dann der Eintrag im Stammzertifikat herangezogen. Das CA-Zertifikat enthält Informationen darüber, ob das Zertifikat der Gegenstelle gültig ist oder nicht. Das CA-Zertifikat steht in Dateiform (CRT-Datei) zur Verfügung und ist auf den Router zu importieren.



Bezeichnung	Funktion/Beschreibung
Neues Zertifikat importieren	**CRT-Datei auswählen:** Manuelle Eingabe des Speicherortes oder durchsuchen des entsprechenden Laufwerkes nach der Zertifikatsdatei. (Dateinamen-Erweiterung: .crt) **Name für dieses Zertifikat (optional):** Optionale Eingabe des Namens für die Zertifikatsdatei. Wird kein Name angegeben, dann wird automatisch der generelle Name (Common Name) verwendet. **CRT-Datei importieren:** Falls die obigen Einstellungen korrekt eingegeben sind, kann die Zertifikatsdatei hiermit importiert werden.
Liste der importierten Zertifikate	Hier werden die bereits importierten Zertifikate aufgelistet. Weitere Zertifikatsdateien können über *„CRT-Datei importieren"* aufgenommen werden.

7.8.3 Partner Zertifikate

Partner Zertifikate sind Zertifikate der Gegenstelle. Sie werden nur benötigt, wenn man in den VPN-Einstellungen *„Authentisierung durch Partnerzertifikat“* gewählt hat. Dann gilt als Entscheidungskriterium für die Gültigkeit eines Zertifikates, dass eine Kopie dieses Zertifikates lokal vorliegt. Das Zertifikat der Gegenstelle ist über die entsprechende crt-Datei auszuwählen und dann zu importieren. Es können auch mehrere crt-Dateien importiert werden.

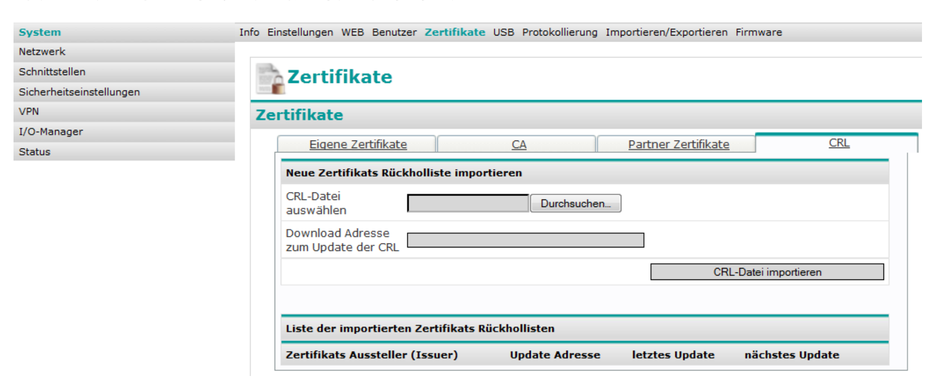


Bezeichnung	Funktion/Beschreibung
Neues Zertifikat importieren	**CRT-Datei auswählen:** Manuelle Eingabe des Speicherortes oder durchsuchen des entsprechenden Laufwerkes nach der Zertifikatsdatei. (Dateinamen-Erweiterung: .crt) **Name für dieses Zertifikat (optional):** Optionale Eingabe des Namens für die Zertifikatsdatei. Wird kein Name angegeben, dann wird automatisch der generelle Name (Common Name) verwendet. **CRT-Datei importieren:** Falls die obigen Einstellungen korrekt eingegeben sind, kann die Zertifikatsdatei hiermit importiert werden.
Liste der importierten Zertifikate	Hier werden die bereits importierten Zertifikate aufgelistet. Weitere Zertifikatsdateien können über *„CRT-Datei importieren“* aufgenommen werden. Weitere Infos zu Namen, Zertifikats Inhaber (Subject), Zertifikataussteller (Issuer), gültig von / bis und Download entnehmen Sie bitte dem Kapitel Eigene Zertifikate.

7.8.4 CRL

Über die Rückhol- und Sperrliste (Certificate Revocation List) wird überprüft, ob die Zertifikate von sich einwählenden Rechner gültig sind oder nicht. Die CRL enthält die Seriennummern von Zertifikaten, die gesperrt werden sollen. Wenn man also Personen, die Be-

rechtigung zur Einwahl auf den Router oder die dahinterliegende SPS entziehen will, so muss lediglich eine CRL erstellt werden. Dies ist mit XCA leicht zu realisieren.

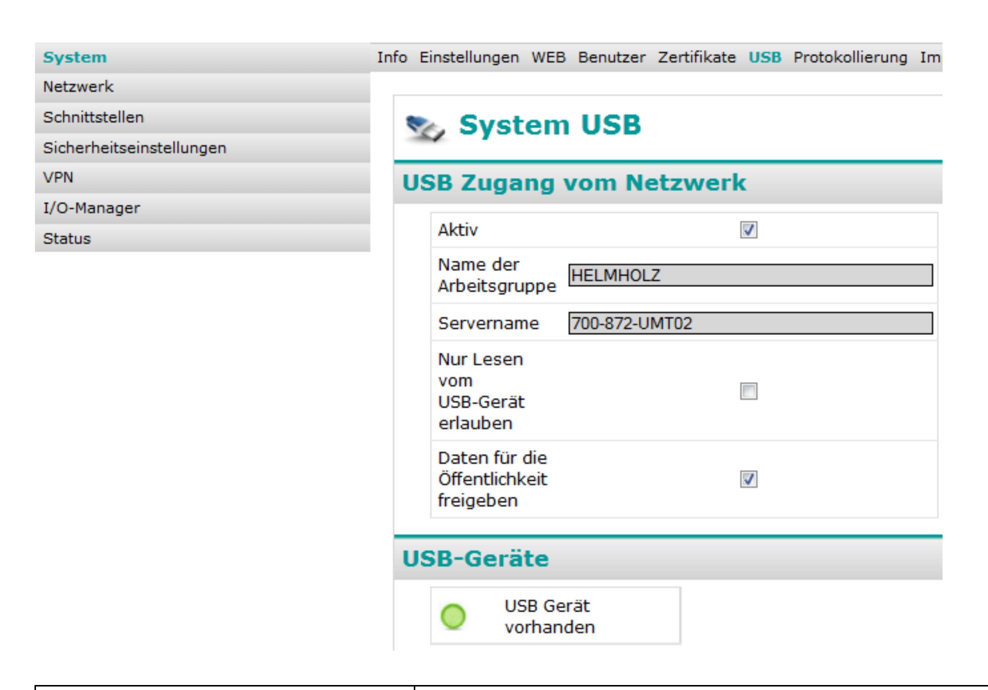


Bezeichnung	Funktion/Beschreibung
Neues Zertifikat importieren	**PEM-Datei auswählen:** Manuelle Eingabe des Speicherortes oder durchsuchen des entsprechenden Laufwerkes nach der Sperrdatei. (Dateinamen-Erweiterung: .pem) **Download Adresse zum Update der CRL:** Die PEM-Datei kann regelmäßig bei Angabe der Download Adresse erneuert werden. **PEM-Datei importieren**: Falls die obigen Einstellungen korrekt eingegeben sind, kann die Sperrdatei importiert werden.
Liste der importierten Zertifikate	Hier werden die bereits importierten Zertifikate aufgelistet. Weitere Zertifikatsdateien können über *„PEM-Datei importieren“* aufgenommen werden.
Update Adresse	Anzeige der Update Adresse für die Sperrdatei.
Letztes Update	Anzeige, wann das letzte Update der Sperrdatei stattfand.
Nächstes Update	Anzeige, wann das nächste Update der Sperrdatei durchgeführt wird.

7.9 System – USB

Am USB Anschluss des REX 300 können Sie ein USB-Gerät (Speicherstick oder USB-Festplatte) anschließen und diese für die Benutzer des Netzwerkes als zusätzliches Laufwerk freigeben. Weiterhin kann der USB Speicher als Protokollierungsspeicher genutzt werden. Eine weitere Funktion des USB Speichers ist das Importieren von Konfigurationen, die auf einem USB Speicher abgelegt wurden.

Zur Einrichtung des USB-Anschlusses betätigen Sie in der linken Navigationsleiste den Button „System“ und in der oberen Navigationsleiste den Button „USB“. Es wird nachfolgende Bildschirmmaske angezeigt.

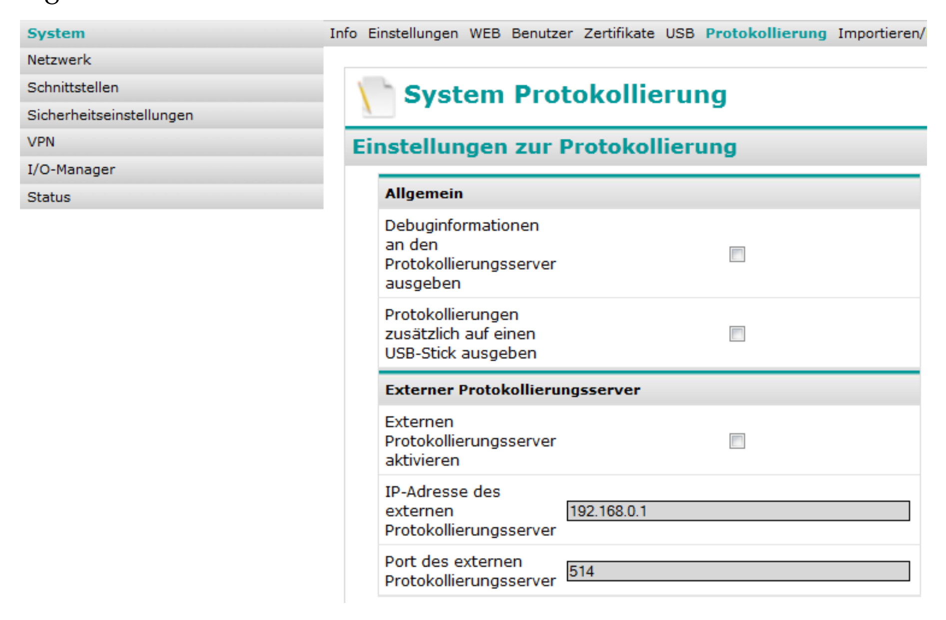


Bitte beachten Sie, dass die Speichermedien den Dateisystemtyp FAT/FAT32 besitzen müssen. Mit anderen Dateisystemen wie z. B. NTFS kann es zu Problemen kommen.

Bezeichnung	**Funktion/Beschreibung**
Aktiv	Wählen Sie hier aus, ob ein angeschlossener USB-Speicher vom REX 300 eingebunden werden soll.
Name der Arbeitsgruppe	Tragen Sie hier den Namen der Arbeitsgruppe ein, über die die Benutzer auf den Speicher zugreifen können.
Servername	Tragen Sie einen Namen ein, unter dem der USB-Speicher in der oben angegebenen Arbeitsgruppe erscheint.
Nur lesen vom USB-Gerät erlaubt	Wählen Sie aus, ob die Benutzer auf den USB-Speicher nur lesend zugreifen dürfen, oder auch auf den USB-Speicher Daten abspeichern können.
Daten für Öffentlichkeit freigeben	Legen Sie fest, ob Benutzern im Netzwerk, die nicht in der Benutzerverwaltung des REX 300 eingetragen sind, der Zugriff auf den USB-Speicher erlaubt sein soll.
USB-Geräte	Im unteren Bereich der Bildschirmmaske wird angezeigt, ob ein USB-Gerät angeschlossen ist. Falls ein USB-Gerät angeschlossen ist, wird dieses symbolisch durch einen grün ausgefüllten Kreis dargestellt.

7.10 System – Protokollierung

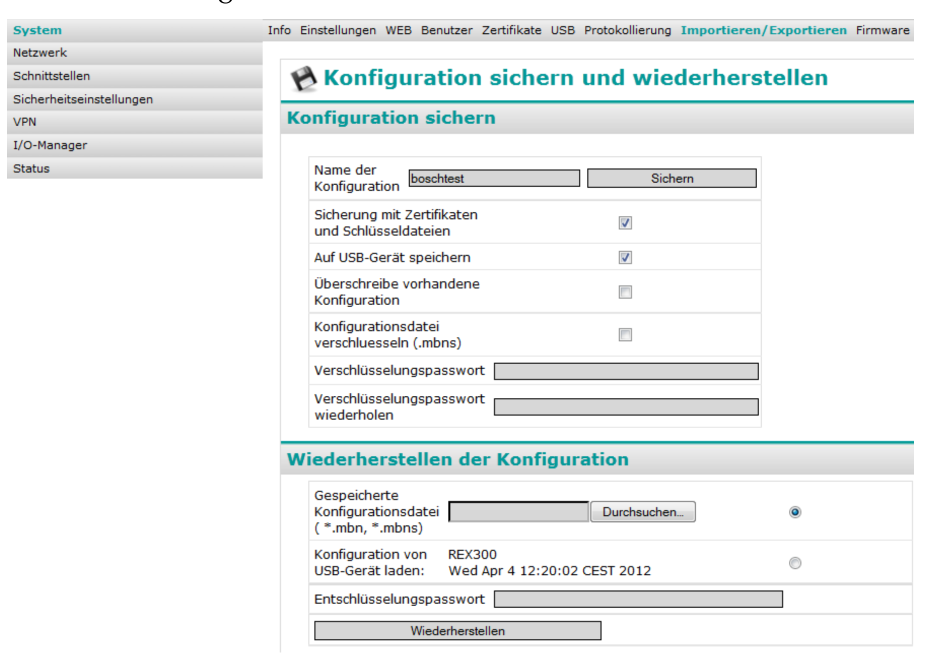
Mithilfe eines Protokollierungsservers (Syslog-Server) kann die Systemprotokollierung des REX 300 auf einen anderen Rechner ausgelagert werden.



Bezeichnung	Funktion/Beschreibung
Debuginformationen an den Protokollierungsserver ausgeben	Eine erweitertes Protokoll wird an den Protokollierungsserver übertragen.
Protokollierung zusätzlich auf einem USB-Stick ablegen	Mit dieser Option wird die Protokollierung zusätzlich auf einem angeschlossenen gespeichert.
Externen Protokollierungsserver aktivieren	Zur Auswahl eines Protokollierungsservers ist die Checkbox durch einen Mausklick mit einem Haken zu versehen. Hiermit kann die Systemprotokollierung des Industrierouters REX 300 auf einen anderen Rechner ausgelagert werden.
IP-Adresse des Protokollierungsservers	IP-Adresse des Protokollierungsservers: Hier: 192.168.0.1
Port des externen Protokollierungsservers	Portangabe des Protokollierungsservers. Hier: 514 Wir empfehlen diesen Port nicht zu ändern, es sei denn, Sie haben eine Anwendung, die auf einen anderen Port reagiert.

7.11 System – Importieren / Exportieren

Die Systemkonfiguration kann hiermit sowohl gespeichert, als auch wiederhergestellt werden.

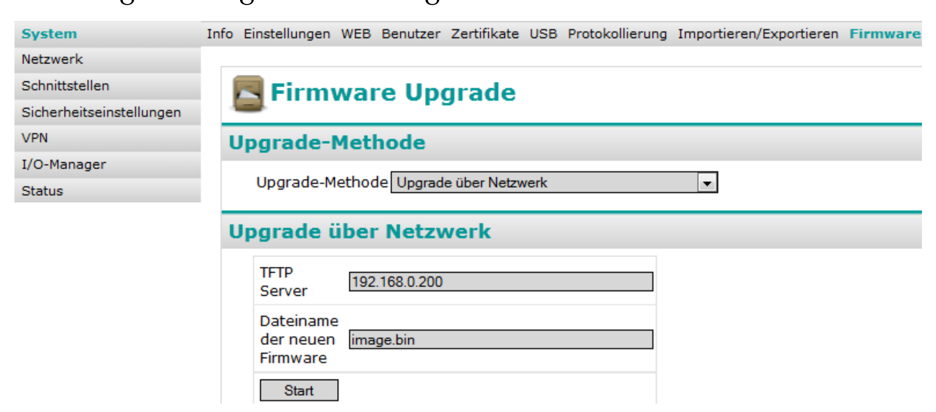


Bezeichnung	Funktion/Beschreibung
Name der Konfiguration	Vergabe eines, für Ihre Anwendung, sinnvollen Namens für die Konfiguration. Standard: REX300
Sichern	Konfiguration sichern. Nach Betätigen des Buttons wird man aufgefordert, den Ort z. B. Laufwerksbuchstabe eines USB-Speichermediums anzugeben.
Sicherung mit Zertifikaten und Schlüsseldateien	Hiermit wird eine Konfiguration angelegt, um einen REX300 zu kopieren. Bitte beachten Sie, dass diese Konfigurationsdatei nur für ein Gerät verwendet wird.
Auf USB-Gerät speichern	Falls ein USB Speichermedium am REX 300 angeschlossen ist, so kann die Konfiguration auch dort gespeichert werden.
Überschreibe vorhandene Konfiguration	Ist die Möglichkeit nicht aktiviert und ist eine Konfigurationsdatei schon an demselben Speicherort vorhanden, dann wird die neue Konfiguration nicht gespeichert. Entweder Sie benennen eine der Dateien um, oder benutzen einen anderen Speicherort für die neue Konfigurationsdatei.

Konfigurationsdatei verschlüsseln (.mbns)	Die gespeicherte Datei wird mit dem angegebenen Passwort verschlüsselt und ist somit nicht mehr als Klartext lesbar.
Verschlüsselungspasswort	Geben Sie hier ein Passwort für die Verschlüsselung der Konfigurationsdatei an.
Gespeicherte Konfigurationsdatei (.mbn, .mbns)	Zum Wiederherstellen einer Konfiguration muss die entsprechend gespeicherte Datei, in der die Konfiguration des Industrierouters enthalten ist, zurück auf den Router übertragen werden. Zum Wiederherstellen ist zuerst die Schaltfläche „*Durchsuchen*" zu betätigen, danach Speicherort bzw. Verzeichnis, in dem sich die Datei befindet, auszuwählen und daraufhin die Taste „*Wiederherstellen*" zu betätigen.
Konfiguration von USB-Gerät laden	Ist eine Konfigurationsdatei auf dem am REX 300 angeschlossenen USB Speichermedium vorhanden, dann wird wie oben im Beispiel die Datei(en) angezeigt. Sie können dann eine der Dateien anwählen und „Wiederherstellen" betätigen. Im Anschluss daran werden Sie gefragt, welche Bereiche der Konfiguration wiederhergestellt werden sollen. Aktivieren Sie die gewünschten Bereiche und bestätigen Sie den Vorgang. Zuletzt werden Sie aufgefordert, das Gerät neuzustarten.
Entschlüsselungspasswort	Wenn Sie eine verschlüsselte Konfigurationsdatei einspielen wollen, müssen Sie hier das entsprechende Passwort zur Entschlüsselung eintragen.
Wiederherstellen	Konfiguration wiederherstellen. Nach Betätigen des Buttons werden Sie gefragt, welche Bereiche der Konfiguration Sie wiederherstellen möchten. Aktivieren Sie die gewünschten Bereiche und bestätigen Sie den Vorgang. Zuletzt werden Sie aufgefordert, das Gerät neuzustarten.

7.12 System – Firmware

Die Aktualisierung der Firmware auf dem Industrierouter kann wie nachfolgend dargestellt durchgeführt werden.



Bezeichnung	Funktion/Beschreibung
Upgrade-Methode	Nach Anklicken des Auswahlfeldes stehen folgende zwei Möglichkeiten der Firmwareaktualisierung zur Verfügung: **Upgrade über USB:** Hierbei muss ein USB-Speichergerät am Industrierouter angeschlossen sein, damit die Datei auf den Industrierouter übertragen werden kann. Hier ist der Firmwarename (Name lautet „image.bin“) eingetragen. Zum Übertragen der Firmware ist die Schaltfläche Start zu betätigen. Danach müssen Sie das Gerät neu starten. **Upgrade über Netzwerk:** Nach einem Mausklick auf das Auswahlfeld müssen Sie *„Upgrade über Netzwerk“* auswählen. Hierbei muss die IP-Adresse eines TFTP-Servers und der Firmwarename (Dateiname) eingetragen werden. Bevor das Upgrade beginnen kann, muss das Tool „tftp32“ gestartet werden. Dies kann auf der Seite http://tftp32.jounin.net/ kostenlos heruntergeladen werden. Nach dem Start des Programms müssen noch einige Einstellungen kontrolliert werden. Im Auswahlfeld *„Current Directory“* muss der Ordner gewählt werden, in dem die Firmwaredatei für das Firmwareupgrade abgelegt ist. Das Tool darf während des Upgrades nicht geschlossen werden.

!

UNTERBRECHEN SIE NIEMALS DEN REX 300 WÄHREND EINER ERNEUERUNG DER FIRMWARE! Das Gerät kann sonst nicht mehr starten.

	Nun muss auf der Weboberfläche die Adresse des Computers, auf dem tftp32 gestartet ist, in das Feld TFTP-Server eingetragen werden. Drücken Sie nun auf die Schaltfläche *„Start“* auf der Weboberfläche. Nachdem der REX 300 mit dem Upgrade fertig ist, muss das Gerät neu gestartet werden.
TFTP-Server	IP-Adresse des Computers, auf dem die tftp32 Software läuft.
Dateiname der neuen Firmware	Angabe des Dateinamens der neuen Firmwaredatei.
Start	Startet den Upgradeprozess

8 Netzwerk

8.1 Netzwerk – LAN

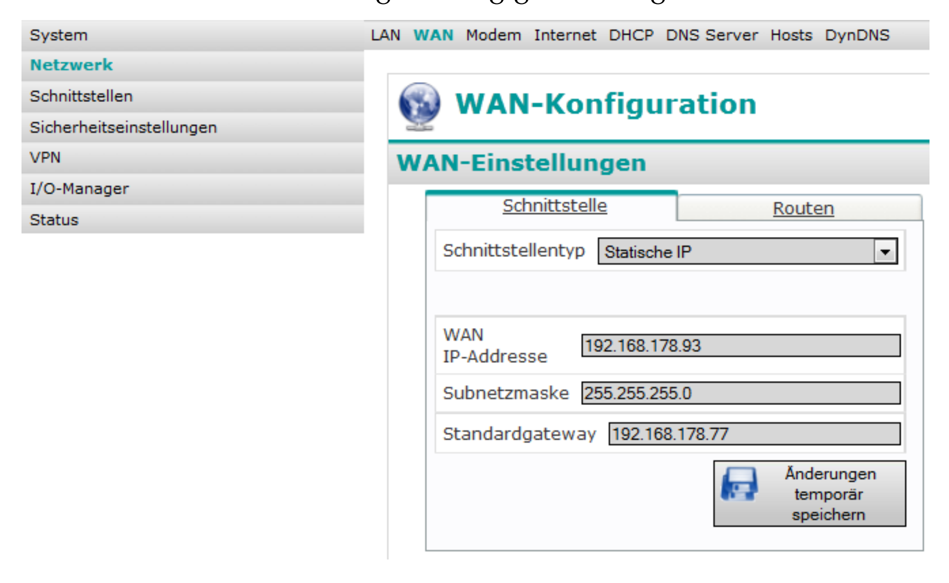
Über die LAN-Konfiguration lässt sich die IP-Adresse (LAN-Adresse) und die Subnetzmaske des Routers konfigurieren. Über diese IP-Adresse ist der Router im LAN-Netzwerk erreichbar.



Bezeichnung	Funktion/Beschreibung
Schnittstelle	Zur Einstellung der LAN-Schnittstelle ist die Registerkarte auszuwählen.
LAN-IP-Adresse	Eintrag der entsprechenden IP-Adresse des Routers.
Subnetzmaske	Eintrag der Subnetzmaske des entsprechenden Netzwerkes, in dem der Router integriert werden soll
Routen	Zur Einstellung bestimmter Routen ist die Registerkarte Routen anzuklicken. Hier können sowohl Netzrouten in CIDR-Form (x.x.x.0/24) als auch Hostrouten angegeben werden.

8.2 Netzwerk – WAN

Die WAN-Schnittstelle des Industrierouters kann ein lokales Netzwerk mit einem weiteren Netzwerk oder dem öffentlichen Netzwerk, wie z. B. das Internet, verbinden. Die WAN-Schnittstelle ist deshalb hierzu anwendungsabhängig zu konfigurieren.



Bezeichnung	Funktion/Beschreibung
Schnittstellentyp	Folgende Schnittstellentypen können ausgewählt werden:
	DSL: Wählen Sie diese Option, wenn Ihr Router direkt mit einem DSL-Modem verbunden ist, das die Verbindung ins Internet herstellt.
	DHCP: Wählen Sie diese Einstellung, wenn ein DHCP-Server im Netzwerk vorhanden ist und somit der Industrierouter automatisch eine IP-Adresse zugewiesen bekommt. **Wenden Sie sich diesbezüglich auch an Ihren Netzwerkadministrator.**
	Statische IP: Wählen Sie diese Einstellung, wenn ein bereits vorhandener Router die Verbindung ins Internet herstellt und dieser nicht als DHCP-Server arbeitet, bzw. keine Adressenvergabe durch einen Server vorgegeben ist. Diese Einstellung ist auch zu wählen, wenn Sie von Ihrem ISP eine statische Adresse erhalten, haben z. B. bei einer Standleitung. Weiterhin muss beachtet werden, dass bei dieser Art der Verbindung ein DNS-Server

<table>
<tr><td rowspan="4"></td><td colspan="2">eingetragen werden muss (siehe Kapitel Netzwerk – DNS-Server)</td></tr>
<tr><td>WAN-IP-Adresse</td><td>IP-Adresse des Routers am WAN-Anschluss</td></tr>
<tr><td>Subnetzmaske</td><td>Eingabe der Subnetzmaske</td></tr>
<tr><td>Standardgateway</td><td>Geben Sie hier das entsprechende Gateway ein, das Sie mit dem Internet verbindet, also die IP-Adresse des bestehenden Routers</td></tr>
<tr><td rowspan="3">Verbindungsmodus</td><td colspan="2">Bei Auswahl des Schnittstellentyps DSL ist zusätzlich eine der nachfolgenden Optionen auszuwählen.</td></tr>
<tr><td colspan="2">PPPoE:
Wählen Sie diese Option aus, wenn Ihr Internetserviceprovider eine PPPoE-Verbindung (Point-To-Point Protocol over Ethernet) erfordert. Diese Option wird bei vielen Modems eingestellt. Die externe IP-Adresse, unter der der Router von einer entfernten Gegenstelle aus erreichbar ist, wird vom Internetprovider festgelegt. Bitte entnehmen Sie die notwendigen Informationen den Unterlagen Ihres Providers.
PPP Benutzer:
Geben Sie hier Ihren Benutzernamen ein. Entnehmen Sie den Benutzernamen den Zugangsdaten Ihres Providers.
PPP Passwort:
Geben Sie hier Ihr Passwort ein. Entnehmen Sie das Passwort den Zugangsdaten Ihres Providers.</td></tr>
<tr><td colspan="2">PPTP:
Wählen Sie diese Option aus, wenn Ihr Internetserviceprovider eine PPTP-Verbindung (Point-To-Point Tunneling Protocol) erfordert. In Österreich wird z. B. PPTP zur DSL-Anbindung verwendet.
PPP Benutzer:
Entnehmen Sie den Benutzernamen den Zugangsdaten Ihres Internetdienstanbieters.
PPP Passwort:</td></tr>
</table>

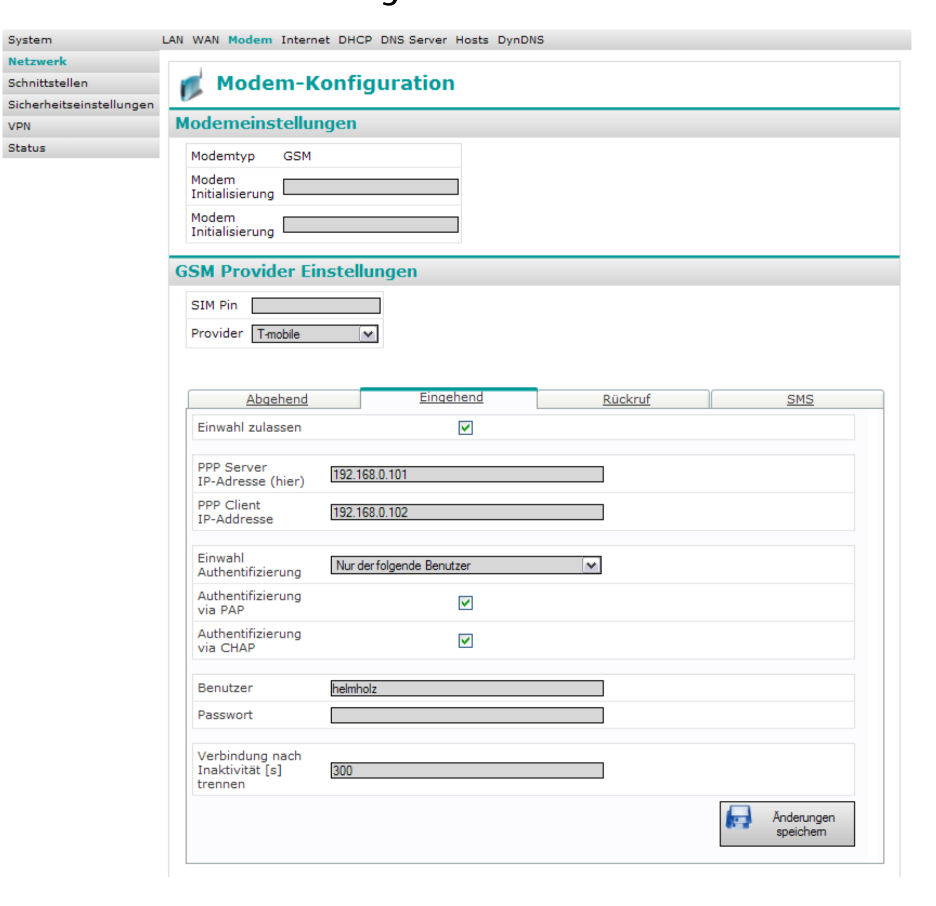
	Entnehmen Sie das Passwort den Zugangsdaten Ihres Internetdienstanbieters. **WAN-IP-Adresse:** Geben Sie hier die IP-Adresse des Routers am WAN-Anschluss ein. Es handelt sich hierbei um eine Adresse, unter der der Router von Geräten erreichbar ist, die sich auf der Seite des WAN-Anschlusses befinden. Falls Ihnen die IP-Adresse Ihres Internet Service Providers nicht automatisch zugewiesen wird, tragen Sie hier die IP-Adresse, unter der der Router vom PPTP-Server aus erreichbar ist, manuell ein. Bitte entnehmen Sie die notwendigen Informationen den Unterlagen Ihres Providers. **Subnetzmaske:** Tragen Sie hier die Netzmaske des am LAN-Anschluss angeschlossenen Netzwerkes ein. **PPTP Server IP-Adresse:** Tragen Sie hier die IP-Adresse des Servers Ihres Internet Providers ein.
Routen	Optional können hier Routen zu anderen Netzwerken definiert werden. Sind am lokal angeschlossenen Netz weitere untergeordnete Netze angeschlossen, können Sie hier zusätzliche Routen definieren. Hier können sowohl Netzrouten in CIDR-Form (x.x.x.0/24) oder Routen zu einzelnen Netzteilnehmern angegeben werden.

8.3 Netzwerk – Modem

8.3.1 Netzwerk-Modem-Eingehend

!

Die Funktion „Eingehend“ ist nicht mit allen Modemvarianten verfügbar!





Bitte beachten Sie, dass Sie Modembefehle immer ohne das vorangestellte „AT“ eintragen!

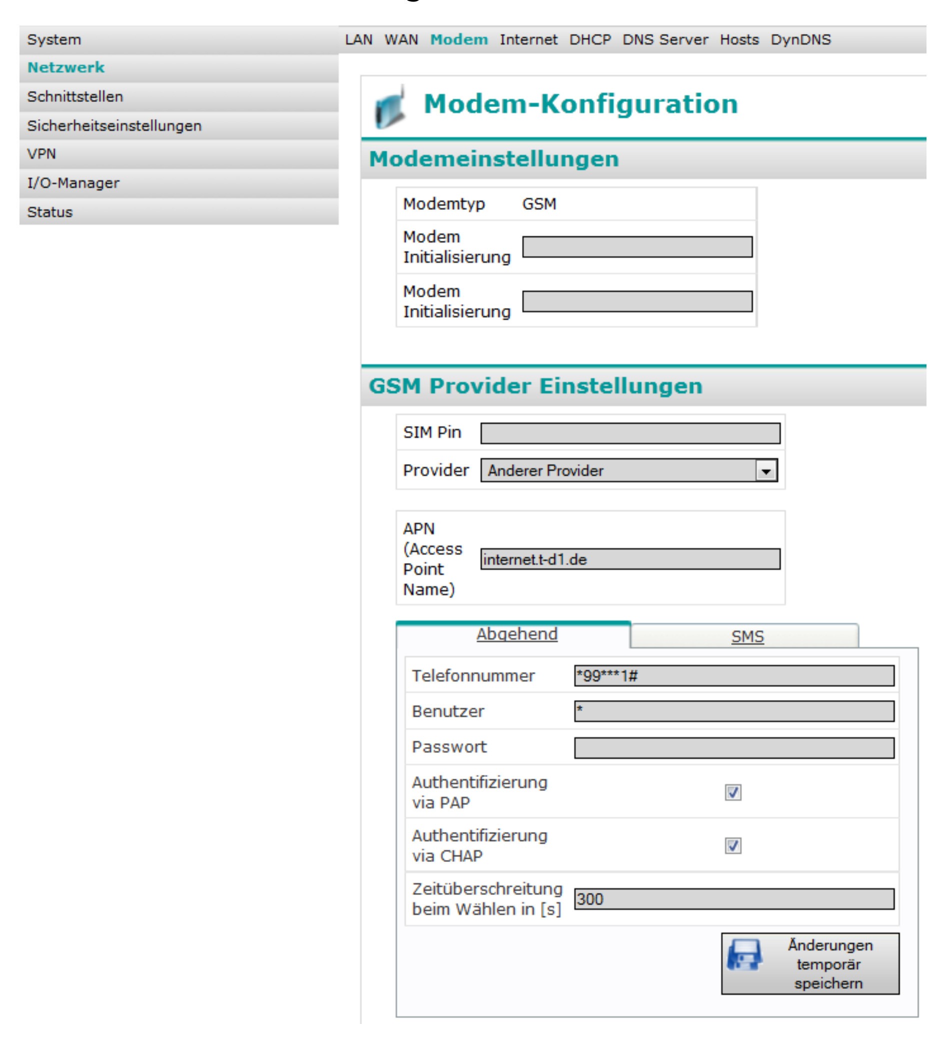
Bezeichnung	Funktion/Beschreibung
Modem Initialisierung	**ANALOG:** Wenn Sie ein analoges Gerät verwenden, dann müssen Sie hier den Befehl +GCI=Ländercode (Ländercode siehe Kapitel Ländercodes für analoge Geräte) und in die zweite Zeile den Befehl X3 (nicht auf Freizeichen warten) eingeben. **ISDN:** Wenn Sie ein ISDN-Gerät verwenden, dann müssen Sie mit dem Befehl AT#Z=n (n=MSN Nummer) ihre MSN-Nummer eingeben. Geben Sie für „n“ einen „*“ ein, dann wird jeder Anruf angenommen. **GSM:** Wenn Sie ein GSM-Gerät verwenden, dann müssen Sie nur den voreingestellten Befehl X3 beibehalten. Der Befehl +GCI=Ländercode darf nicht ver-

	wendet werden.
SIM-PIN (nur bei GSM)	Hier kann, falls notwendig, der PIN für die SIM-Karte eingegeben werden.
Provider	Hier kann der Mobilfunkanbieter ausgewählt werden. Falls der Anbieter nicht dabei ist, können Sie den APN (Access Point Name) Ihres Providers auch von Hand eingeben. Informationen zum APN bekommen Sie von Ihrem Mobilfunkanbieter.

Bezeichnung	**Funktion/Beschreibung**
Eingehend	Um analoge oder digitale (ISDN) Einwahlverbindungen auf dem Router zu ermöglichen, ist diese Option zu aktivieren.
Einwahl zulassen	Die Funktion müssen Sie durch einen Mausklick mit einem Haken versehen, um den Zugriff von einem Clientcomputer auf den Router freizugeben.
PPP-Server IP Adresse (lokal)	Hier ist die IP-Adresse des Routers einzutragen. Es ist möglich, den gleichen Netzbereich, wie den des lokalen Netzes zu verwenden. Achten Sie aber bitte darauf, dass die vergebenen Adressen nicht nochmals benutzt werden. Andernfalls kann es zu Adressenkonflikten kommen.
PPP-Client IP-Adresse	Hier ist die IP-Adresse einzutragen, die der Router dem Client (anrufende Gegenstelle) zuteilt, sobald eine PPP-Verbindung zustande gekommen ist. Der Router und die Gegenstelle bilden somit nach dem Verbindungsaufbau ein eigenes Netzwerk.

Einwahl Authentifizierung	Stellen Sie hier ein, ob für die Einwahl auf den Router eine Abfrage von Benutzername und Passwort (sog. Authentifizierung) erforderlich ist. Folgende Auswahlen sind möglich:
	Nur der folgende Benutzer: Nur der in den nachfolgenden Eingabefeldern eingetragene Benutzer ist berechtigt, eine Einwahl auf den Router durchzuführen.
	Jeder Benutzer mit Einwahlrechten: Jeder Benutzer, der im Benutzermanagement mit „Modem"-Rechten eingetragen wurde, ist berechtigt, eine Verbindung aufzubauen.
Authentifizierung via PAP/CHAP	Übernehmen Sie die werksseitige Voreinstellung. PAP/CHAP sind die Authentifizierungsarten. Gleichen Sie diese Einstellung mit der des einwählenden Partners ab. Eine Deaktivierung von PAP/CHAP, hat zur Folge, dass diese Authentifizierung nicht akzeptiert wird und ihre gesendeten Daten auch für Andere lesbar sind.
Benutzername & Passwort	Geben Sie hier den Benutzernamen und das zugehörige Passwort für die PPP-Einwahl ein. Diese Felder sind nur vorhanden, wenn die Option *„Nur der folgende Benutzer"* bei *„Einwahl Authentifizierung"* gewählt wurde.
Verbindung nach Inaktivität [s] trennen	Hier ist die Zeit anzugeben, nach der eine bestehende Verbindung abgebaut wird, wenn während dieser Zeit keine Datenpakete übertragen werden. Falls nichts eingegeben wird, oder eine „0" eingetragen ist, wird die Verbindung nicht abgebaut.

8.3.2 Netzwerk-Modem-Ausgehend

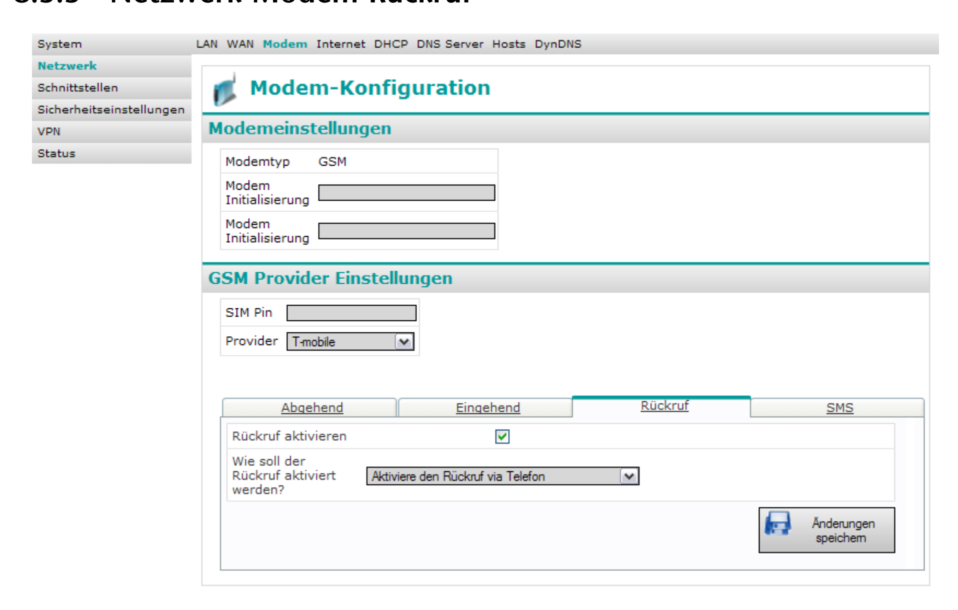


Die nachfolgenden Einstellungen beziehen sich auf ausgehende Verbindungen des Modems.

Bezeichnung	Funktion/Beschreibung
Telefonnummer	Geben Sie hier die Rufnummer des entsprechenden Providers ein. Bei GSM-Modems lautet diese Nummer stets *99***1#.
Benutzer	Geben Sie den Benutzernamen ein, der zur Einwahl beim entsprechenden Anbieter erforderlich ist. Weitere Infos hierzu erhalten Sie direkt bei Ihrem Anbieter.
Passwort	Geben Sie das Passwort ein, das zur Einwahl beim entsprechenden Anbieter erforderlich ist. Weitere Infos hierzu erhalten Sie direkt bei Ihrem Anbieter.

Authentifizierung via PAP	Übernehmen Sie das standardmäßig eingestellte Authentifizierungsprotokoll. Dies ist bei der Einrichtung einer DFÜ-Verbindung grundsätzlich vorein-gestellt.
Authentifizierung via CHAP	Übernehmen Sie das standardmäßig eingestellte Authentifizierungsprotokoll. Dies ist bei der Einrichtung einer DFÜ-Verbindung grundsätzlich vorein-gestellt. CHAP ist im Regelfall das Ver-fahren, das bei der Anmeldung an den Internetzugang beim Internetdienstean-bieter (ISP) per Modem oder ISDN-Adapter durchgeführt wird.
Zeitüberschreitung beim Wählen in [s]	Nach dieser eingestellten Zeit wird der Wählversuch abgebrochen und eine erneute Anwahl gestartet.

8.3.3 Netzwerk-Modem-Rückruf

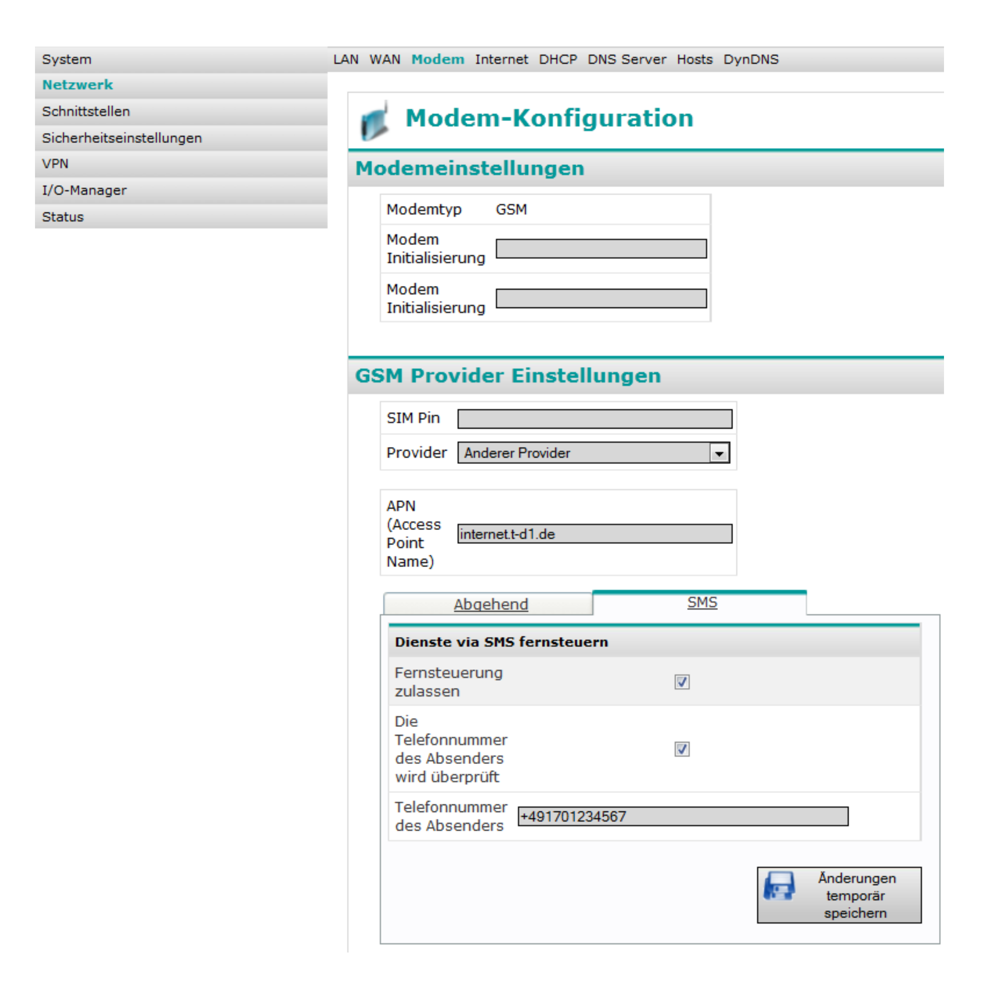


Die nachfolgenden Einstellungen beziehen sich auf die Rückruffunktion. Diese Funktion dient dazu, den Vorgang für die Einwahl ins Internet von außen durch einen Telefonanruf bzw. DFÜ-Verbindung zu starten. Es muss eingestellt werden, dass die Internetverbindung via WAN oder via Modem aufgebaut wird. Damit die Rückruffunktion genutzt werden kann, muss der REX 300 in den Wartezustand gebracht werden. (nur Analog-Geräte)

Bezeichnung	Funktion/Beschreibung
Rückruf aktivieren	Wenn Sie diese Option markieren, können Sie den Rückruf ermöglichen.
Wie soll der Rückruf aktiviert werden?	**Aktiviere den Rückruf via Telefon:** Wenn Sie diese Einstellung wählen, verbindet sich der REX 300 ins Internet, wenn er von einem Telefon angerufen wird. Damit die Verbindung aufgebaut werden kann, muss der REX 300 mit viermaligem Klingeln darauf aufmerksam gemacht werden. Im Anschluss daran legt der REX 300 auf und startet den Vorgang für eine Einwahl in das Internet. Dies kann 30-40 Sek. dauern.

	Einloggen und Button klicken: Wenn Sie diese Einstellung wählen, verbindet sich der REX 300 ins Internet, wenn Sie eine DFÜ-Verbindung zum REX 300 aufgebaut haben und auf der Benutzeroberfläche im Menü „**System – Info**“ auf den Button „*Call Back*“ klicken. Nachdem dies geschehen ist, haben Sie 30 Sekunden Zeit die DFÜ-Verbindung wieder zu trennen, denn danach baut der REX 300 die Verbindung ins Internet auf.

8.3.4 Netzwerk-Modem-SMS



!

Bitte beachten Sie, dass die angegebene Mobilfunknummer nicht mit einer Null beginnen darf. Geben Sie statt der Null z. B. für Deutschland +49 ein!

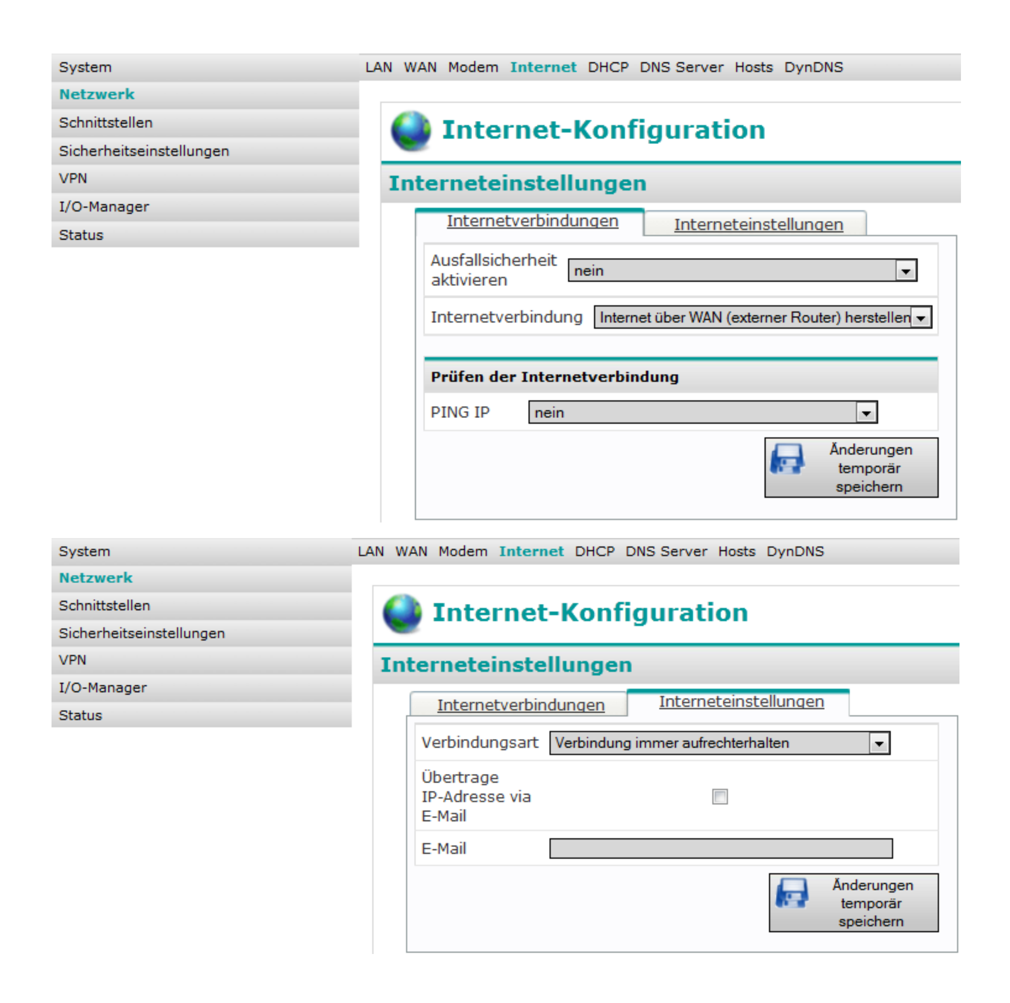
Bezeichnung	**Funktion/Beschreibung**
Fernsteuerung zulassen	Mit dieser Funktion wird die Steuerung durch Kurznachrichten aktiviert.
Die Tel. Nr. des Absenders wird überprüft	Hiermit wird sichergestellt, dass der REX 300 nur Befehle per Kurznachrichten annimmt, die von einer bestimmten Nummer kommen. Jetzt müssen Sie noch die Telefonnummer des Absenders im Feld „*Telefonnummer des Absenders*“ direkt darunter eingeben. Kommen Befehle von einer anderen Nummer, dann werden diese ignoriert.

Liste möglicher SMS-Befehle:

Befehl	**Wirkung**
INET START	Der REX 300 baut eine Internetverbindung auf. (Modemverbindung)
INET STOP	Der REX 300 wird dann die Internetverbindung beenden. (Modemverbindung)
IPSEC START [Verbindungsname]	Der REX 300 startet die IPSec Verbindung mit dem Namen x.
IPSEC STOP [Verbindungsname]	Der REX 300 stoppt die IPSec Verbindung mit dem Namen x.
PPTP START [Verbindungsname]	Der REX 300 startet die PPTP Verbindung mit dem Namen x.
PPTP STOP [Verbindungsname]	Der REX 300 stoppt die PPTP Verbindung mit dem Namen x.
OPENVPN START [Verbindungsname]	Der REX 300 startet die OpenVPN Verbindung mit dem Namen x.
OPENVPN STOP [Verbindungsname]	Der REX 300 stoppt die OpenVPN Verbindung mit dem Namen x.
REBOOT	Der REX 300 führt einen Neustart durch.
GSM CMD [AT-Befehl]	Mit dem Befehl GSM CMD [AT-Befehl] ist es möglich, beliebige AT-Befehle an das Modem zu senden. Die Antwort des Modems wird per SMS an die Absenderadresse übermittelt. Es können nur Modemantworten mit maximal 160 Zeichen übertragen werden.

8.4 Netzwerk – Internet

Für die Einwahl des Routers ins Internet ist dieser verbindungsspezifisch und abhängig von bestimmten Ereignissen entsprechend zu konfigurieren.



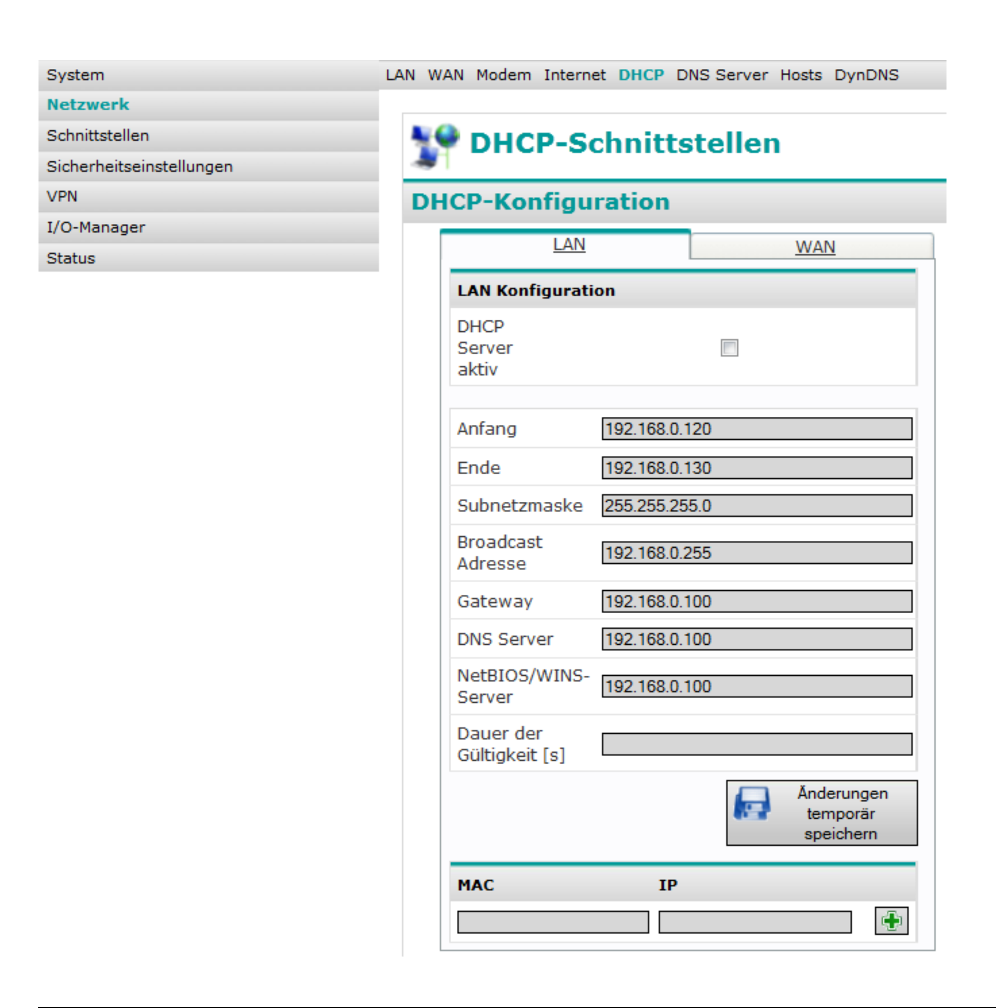
Bezeichnung	Funktion/Beschreibung
Internetverbindung	
Ausfallsicherheit aktivieren	Die Funktion Ausfallsicherheit ermöglicht das umschalten zwischen verschiedenen Internetverbindungen. Ist diese Funktion aktiviert, können je nach Gerätetyp die Internetschnittstellen in der gewünschten Priorität eingetragen werden.
Internetverbindung	Folgende Möglichkeiten stehen über das Auswahlfeld zur Verfügung:
	Internet über WAN (externer Router) herstellen: Wählen Sie diese Einstellung, wenn der REX 300 nicht selbst eine Internetverbindung herstellen soll. Das trifft z. B. zu, wenn in Ihrem Netzwerk ein weite-

	rer Router vorhanden ist, der für die Internetverbindung zuständig ist, oder wenn nur eine eingehende Wählverbindung über das öffentliche Telefonnetz erfolgen soll.
	Internet über Modem herstellen: Bei dieser Einstellung wird eine Verbindung über das interne Modem aufgebaut. Entsprechende Zugangsdaten sind in den Einstellungen **Netzwerk – Modem** einzutragen.
	Internet über WAN herstellen: Wenn die Internetverbindung z. B. über ein DSL-Modem erfolgen soll, dann ist diese Einstellung auszuwählen. Sie müssen jedoch zusätzlich unter **Netzwerk – WAN** Ihre Internetzugangsdaten eingeben. Starten Sie danach den REX 300 neu, damit die Änderungen wirksam werden.
Prüfen der Internetverbindung	Zusätzlich kann die Verfügbarkeit der Internetverbindung durch das PING'en einer IP-Adresse geprüft werden. Es können bis zu drei unterschiedliche IP-Adressen mit unterschiedlichen Intervallen eingetragen werden.
Interneteinstellungen	
Verbindungsart	**Verbindung immer aufrechterhalten:** Wählen Sie diese Einstellung, wenn der Router beim Neustart oder durch Betätigen des Tasters RESET, an der Oberseite des Routers, sofort versuchen soll, eine Verbindung ins Internet aufzubauen. ACHTUNG! Die Internetverbindung wird nicht getrennt!
	Bei Bedarf: Wählen Sie diese Einstellung, wenn der Router dann eine Verbindung ins Internet aufbauen soll, wenn eine der nachfolgend aufgelisteten Optionen ausgewählt wird: *Verbindung ins Internet durch Betätigen der Taste Dial Out* *Verbindung bei Datentransfer*
Übertrage IP-Adresse via E-Mail	Hier können Sie einstellen, ob eine E-Mail mit der aktuellen öffentlichen IP-Adresse an eine vorher eingetragene E-Mail-Adresse gesendet werden soll.

E-Mail	Falls die Option *„IP via E-Mail versenden“* gewählt wurde ist hier Ihre E-Mail-Adresse anzugeben. Sie können per Hand auch mehrere E-Mail-Adressen durch ein Semikolon getrennt angeben.
Standard Netzwerkroute	Ist die Standard Route über [Modem] gewählt, so wird als Standardgateway immer die Internetverbindung über das Modem benutzt. Die Standard Route über [WAN Ethernet] verwendet als Standardgateway immer den Weg über die WAN Buchse. In diesem Fall müssen dann explizit entsprechende Routen für den Internetdatenverkehr angegeben werden.
Einstellungen	Die Registerkarte *„Einstellungen“* ist nur dann sichtbar, wenn eine Verbindung zum Internet entweder über WAN oder per Modem ausgewählt wurde, und die Verbindungsart *„Bei Bedarf“* über das Auswahlfeld eingestellt ist. Die nachfolgenden Einstellungsmöglichkeiten werden angezeigt:
Verbindung bei Datentransfer	Soll eine Verbindung ins Internet durch gesendete Datenpakete stattfinden, dann ist die Checkbox mit einem Haken zu versehen. D. h., wenn vom LAN aus versucht wird, einen Teilnehmer zu erreichen, der sich nicht im LAN befindet, dann wird eine Verbindung ins Internet aufgebaut. Z. B., wenn Sie einen Ping auf google.com absetzen.
Verbindung über Taste „Dial Out“	Soll die Verbindung ins Internet durch Betätigen des Tasters *„Dial out“* oberhalb der MPI/PROFIBUS Schnittstelle ausgelöst werden, dann versehen Sie die Checkbox mit einem Haken.
Verbindung nach Inaktivität [s] trennen	Hiermit stellen Sie ein, nach welcher Zeit die bestehende Internetverbindung getrennt werden soll, sobald keine Datenpakete mehr vom Router versandt werden. Wenn Sie das Feld leer lassen, ist diese Funktion deaktiviert.

8.5 Netzwerk – DHCP

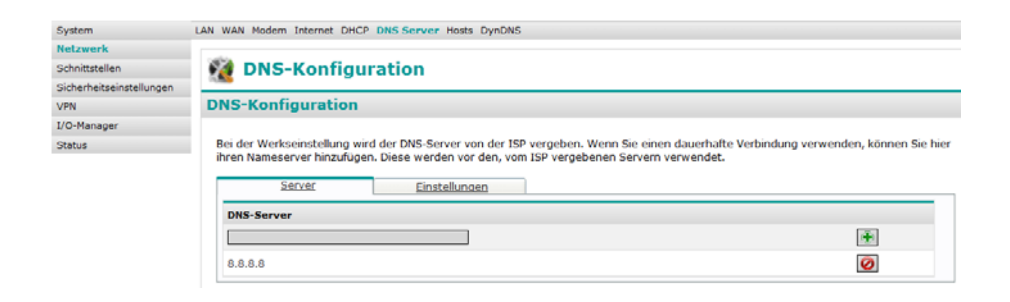
Der Industrierouter kann als DHCP-Server im LAN oder WAN-Netzwerk konfiguriert werden. Durch DHCP ist die Einbindung eines neuen Computers in ein bestehendes Netzwerk ohne weitere Konfiguration möglich. Es muss lediglich der automatische Bezug der IP-Adresse am Computer eingestellt werden.



Bezeichnung	Funktion/Beschreibung
LAN/WAN	Auswahl zur Konfiguration der LAN bzw. WAN-Schnittstelle.
DHCP-Server aktiv	Durch Auswahl dieser Checkbox kann der Router als DHCP-Server an der entsprechenden Schnittstelle aktiviert werden.
Anfang	Hier ist die Anfangsadresse des Adressbereichs einzugeben, der vom DHCP-Server verwaltet wird.
Ende	Endadresse des vom DHCP-Server verwalteten Bereichs.
Subnetzmaske	Subnetzmaske des vom DHCP-Server verwalteten Bereichs.

Broadcast Adresse	Broadcast Adresse des vom DHCP-Server verwalteten Bereichs.
Gateway	Hier kann optional eine Adresse eines Routers eingetragen werden, der im Netzwerk anwesende Clients mit dem Internet oder mit einem anderen Netzwerk verbindet. Ansonsten tragen Sie hier die LAN-IP-Adresse des Routers ein.
DNS-Server	Optionale Eingabe eines im Netzwerk vorhandenen DNS-Servers. Ansonsten tragen Sie hier die LAN-IP-Adresse des REX 300 ein.
NetBIOS/WINS-Server	Optionale Eingabe eines im Netzwerk vorhandenen NetBIOS/WINS-Servers. Ansonsten tragen Sie hier die LAN-IP-Adresse des REX 300 ein.
Dauer der Gültigkeit [s]	Zeitdauer, während ein Client vom DHCP-Server eine bestimmte IP-Adresse zugeteilt bekommt. (Lease Time).
Tabelle MAC/IP	Tragen Sie hier die feste Zuordnung zwischen IP-Adresse und MAC-Adresse ein. D. h., Sie können hier vorgeben, dass ein Gerät mit einer bestimmten MAC-Adresse immer dieselbe IP-Adresse erhält. Bitte achten Sie darauf, dass Sie MAC-Adressen mit Doppelpunkt verwenden müssen: z. B. 00:06:71:19:1E:24

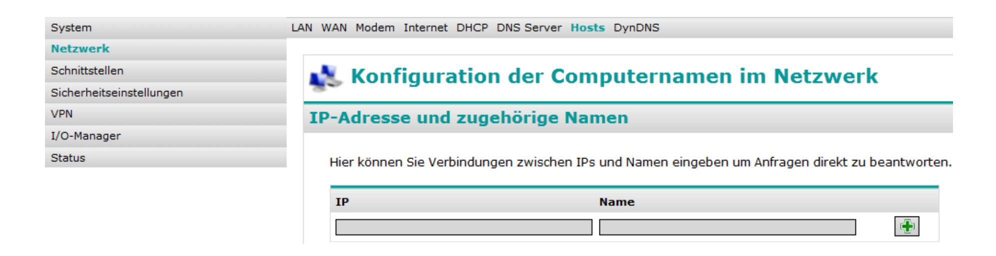
8.6 Netzwerk – DNS-Server



Bezeichnung	**Funktion/Beschreibung**
Server	Nach Auswahl dieser Registerkarte kann ein entsprechender DNS-Server eingetragen werden.
Einstellungen	Nach Anwahl dieser Registerkarte können die nachfolgend aufgelisteten Einstellungen bezüglich DNS-Server aktiviert bzw. eingetragen werden.
Keine Hosts	Die unter Netzwerk-Hosts eingetragenen Computernamen werden nicht berücksichtigt.
Strikte Anordnung	Es wird genau die Reihenfolge der Einträge wie unter *„Servers“* eingehalten.
Filter WIN2K	Filtert ständige und unnötige Anfragen von Windowsclients. Bei einer Internetverbindung *„Bei Bedarf“* ist diese Einstellung sinnvoll, dadurch wird nicht bei jeder Anfrage eine Internetverbindung aufgebaut.
Domain	Sie können hier ein sogenanntes Domainsuffix eintragen.
Speichergröße	Geben Sie hier die Anzahl der gespeicherten Namen an. D. h. wie viele Namen mit IP-Adressen zwischengespeichert werden.

8.7 Netzwerk – Hosts

Über diese Einstellung kann immer genau einer IP-Adresse ein bestimmter Name zugeordnet werden, um DNS-Anfragen direkt beantworten zu können. Über die Eingabefelder können IP-Adressen und zugehöriger Name eingetragen und abgespeichert bzw. gelöscht werden. Der REX 300 muss somit nicht einen anderen DNS-Server befragen, sondern beantwortet die Anfrage direkt.



8.8 Netzwerk – DynDNS

8.8.1 Allgemeines

Da der Industrierouter REX 300 bei einer Einwahl ins Internet eine eindeutige IP zugewiesen bekommt, kann er von einem Client-PC anhand dieser IP gefunden werden. Sobald er aber wieder die Verbindung ins Internet unterbricht und sich später wiederum neu einwählt, erhält er eine neue IP-Adresse. Der DynDNS-Dienst dient dazu, den Industrierouter immer unter gleichem Namen erreichen zu können. Er dient zur Umsetzung von IP-Adressen in Namen und umgekehrt.

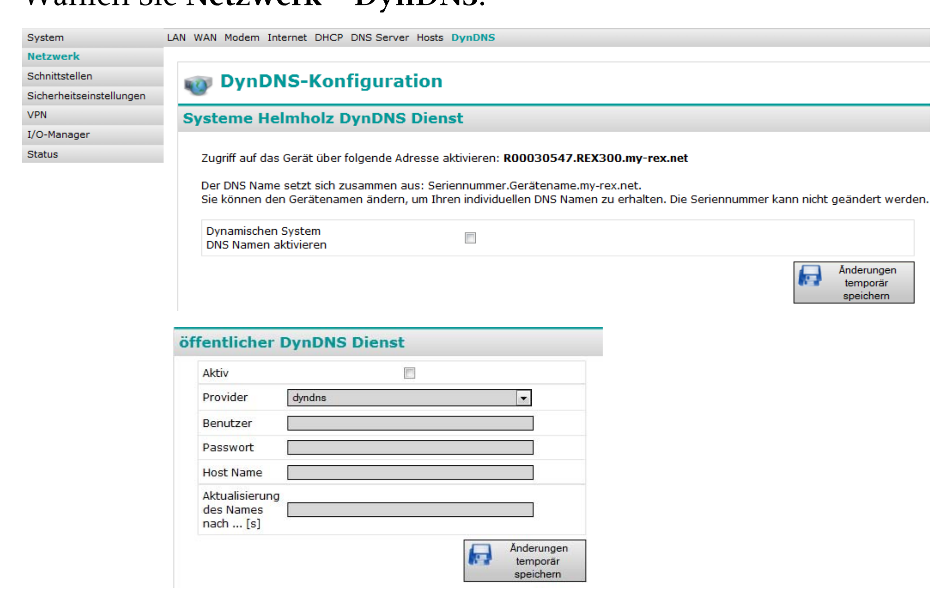
8.8.2 Vorgehensweise zur Einrichtung der DynDNS-Konfiguration

Im REX 300 steht ein automatischer DynDNS Dienst bereit. Dieser DynDNS Dienst wird von der Systeme Helmholz GmbH betrieben. Eine Anmeldung bzw. Registrierung ist nicht erforderlich.

Um einen öffentlichen DynDNS Dienst nutzen zu können, müssen Sie sich zunächst bei einem dieser öffentlichen Dienste registrieren. Diese Registrierung ist in der Regel kostenlos und sollte keine Schwierigkeiten bereiten.

Sofern Sie für einen vom Industrierouter unterstützten DynDNS Dienst registriert sind, können Sie die Eingaben in der nachfolgenden Bildschirmmaske eintragen bzw. auswählen.

Wählen Sie **Netzwerk – DynDNS**.



Systeme Helmholz DynDNS Dienst	
Bezeichnung	**Funktion/Beschreibung**
Dynamischen System DNS Namen aktivieren	Diese Option aktiviert den automatischen DynDNS Dienst der Systeme Helmholz GmbH. Der Namensaufbau ist in diesem Fall fest vorgegeben und kann nur an einer Stelle frei definiert werden: Beispiel: Seriennummer.Gerätename.my-rex.net Die Seriennummer ist fix aber der Gerätename ist frei wählbar. Beispiel: Gerätename: REX300 Seriennummer: R00007805 = Name im Internet: „R00007805.REX300.my-rex.net“ ca. 1-2 Minuten nach Einwahl ins Internet ist der DNS-Name weltweit verfügbar.

!

Bitte beachten Sie, wenn Sie eine Internetverbindung „Bei Bedarf“ verwenden, die Zeit die der DNS Server benötigt, um die IP-Adresse aufzulösen ist in den Timout Einstellungen der Internetverbindung zu berücksichtigen.

Öffentlicher DynDNS Dienst	
Bezeichnung	**Funktion/Beschreibung**
Aktiv	Wenn Sie bei einem DynDNS-Anbieter registriert sind und der Industrierouter diesen Service nutzen soll, dann betätigen Sie die Checkbox, um diese mit einem Haken zu versehen. Der REX 300 meldet somit bei der nächsten Einwahl ins Internet die aktuelle IP-Adresse die er vom Internet-Service-Provider erhalten hat an den DynDNS-Service.
Provider	Wählen Sie hier über das Auswahlfeld den Namen des Anbieters aus, bei dem Sie registriert sind, z. B. dyndns.org.
Benutzer	Geben Sie hier den Benutzernamen ein, den Sie beim DnyDNS-Dienst bei der Registrierung eingegeben haben.
Passwort	Geben Sie das Passwort ein, das Sie beim DynDNS-Dienst für den REX 300 eingegeben haben.
Host Name	Geben Sie hier den Namen an, den Sie beim DynDNS-Dienst für den REX 300 eingegeben haben.
Aktualisierung des Namens nach … [s]	Tragen Sie hier den Intervall zum Aktualisieren des DNS-Namens in Sekunden ein.

9 Schnittstellen

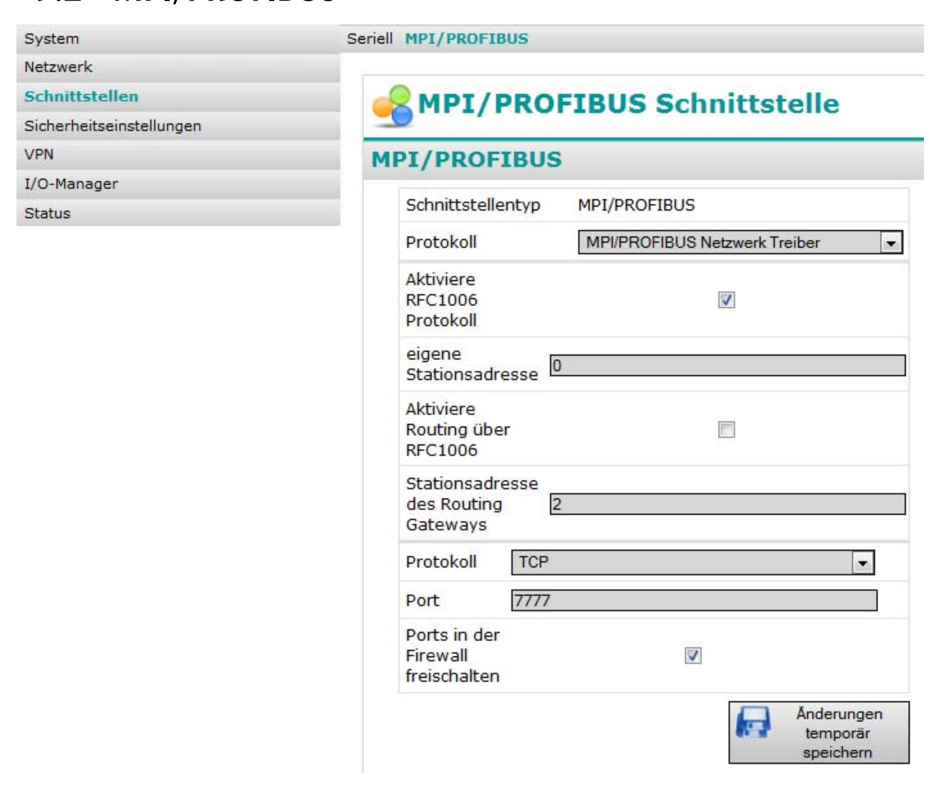
9.1 Seriell



Bezeichnung	Funktion/Beschreibung
Schnittstellentyp	Hier können Sie einstellen, ob die Schnittstelle als eine RS232, eine RS485 oder als RS422 arbeiten soll.
Treiberart	Hier stellen Sie ein, ob der REX einen vordefinierten Treiber aus der Liste der unter (Treiber) verfügbaren Treiber verwenden soll, oder ob eine Benutzerdefinierte Einstellung vorgenommen werden soll.
	Benutzereinstellung: Datenübertragungsrate: Geben Sie hier die Baudrate, mit welcher die Kommunikationsschnittstelle arbeiten soll, an. Datenformat: Wählen Sie die Einstellungen für Datenbits, Parität und Stoppbits. Flusskontrolle: Wählen Sie die Art der Flusskontrolle. Anzahl Empfangsabfragen zur Bildung eines Telegramms: Dies ist ein Empfangszähler für die seriellen Signale. D. h. wie viele Zyklen das System durchläuft bis das Datenpaket abgesendet wird.

Treiber	Wählen Sie den passenden Treiber aus, der für ihre angeschlossenen Geräte passend ist.
Port	Auswahl des Ports für die Netzwerk- oder Internetkommunikation. Wir empfehlen den Standardport 7001 eingestellt zu lassen.
Ports in der Firewall freischalten	Die Checkbox muss aktiviert sein, damit Sie über den eingestellten Port kommunizieren können. Ansonsten werden alle Signale/Pakete geblockt / verworfen. Diese Regel wird jedoch nur angewendet, wenn Sie über die öffentliche Adresse auf die seriellen Schnittstellen zugreifen. Bei einer bestehenden VPN-Verbindung müssen Sie keine Portfreischaltung vornehmen.

9.2 MPI/PROFIBUS



! *Mit der eigenen Stationsadresse meldet sich der angeschlossene Router im MPI/DP Netzwerk an. Dies ist notwendig, wenn Sie ausschließlich die Kommunikation über RFC1006 verwenden. In einem Mischbetrieb von Verbindungen mit Netzwerktreiber und RFC1006 meldet sich der Router immer mit der Adresse an, die in der zuerst genutzten Verbindung angegeben ist.*

! *Soll auf einen Bus-Teilnehmer (Slave) in einem unterlagertem und nicht direkt verbundenen Netzwerk zugriffen werden, muss im Router die Stationsadresse der SPS mit dem Netzübergang (Master) als Routing Gateway eingetragen werden.*

Bezeichnung	**Funktion/Beschreibung**
Aktiviere RFC1006 Protokoll	Hier haben Sie die Möglichkeit die Kommunikation über RFC1006 zu aktivieren.
eigene Stationsadresse	Wenn RFC1006 aktiviert ist und Sie nicht mit unserem NETLink Treiber arbeiten, vergeben Sie hier eine eindeutige MPI/DP Stationsadresse für den Router.
Aktiviere Routing über RFC1006	Diese Option ermöglicht das Routing über RFC1006. Dies wird z. B. für Anwendungen mit projektspezifischer Schnittstelle benötigt. Für weitere Informationen sehen Sie in den entsprechenden Anwendungsbeispielen nach.
Stationsadresse des Routing Gateways	Wenn das Routing über RFC1006 aktiviert ist, muss die Adresse des Routing Gateways eingetragen werden. Beispiel: Die SPS (Master) ist über MPI-Bus (z.B. Adresse 14) mit dem Router (z.B. Adresse 13) verbunden, am Profibus des Masters (z.B. Adresse 4) ist ein Teilnehmer (z.B. Adresse 5) angeschlossen. Um jetzt über den Router (13) per MPI auf den Teilnehmer mit der Adresse 5 am Profibus zuzugreifen muss das Routing aktiviert werden.
Port	Tragen Sie den Port ein, über den Sie die Kommunikation stattfinden lassen wollen.
Ports in der Firewall freischalten	Die Checkbox muss aktiviert sein, damit Sie über den eingestellten Port kommunizieren können. Ansonsten werden alle Signale/Pakete geblockt/verworfen. Diese Regel wird jedoch nur angewendet, wenn Sie über die öffentliche Adresse auf die seriellen Schnittstellen zugreifen. Bei einer bestehenden VPN-Verbindung müssen Sie keine Portfreischaltung vornehmen.

10 Sicherheitseinstellungen

10.1 Sicherheitseinstellungen – Firewall Allgemein

Zum Schutz vor unberechtigten Zugriffen bzw. Verbindungsversuchen besitzt der Industrierouter eine integrierte Firewall. Über diese Firewall wird der kommende und gehende Datenverkehr kontrolliert, protokolliert und freigegeben bzw. gesperrt.

Die Firewall kann allgemein in einer der drei folgenden Varianten betrieben werden:

- Maximalste Sicherheitsstufe
  Die Freigaben für den Datenverkehr müssen entsprechend konfiguriert werden. Sowohl der eingehende und ausgehende Datenverkehr ist gesperrt. Für den Zugriff auf die Weboberfläche (von außen!) muss das TCP-Protokoll und der Zielport 80 bei den Regeln **WAN>LAN** eingetragen und aktiviert werden. Starten Sie jedoch eine VPN-Verbindung, dann wird der Zugriff dementsprechend für die Datenpakete aus dem VPN-Tunnel freigegeben.
- Normale Sicherheitsstufe
  Bei dieser Variante wird der eingehende Datenverkehr (Daten vom Internet) gesperrt, während die ausgehenden Daten akzeptiert werden.
- Minimalste Sicherheitsstufe
  Bei dieser Variante werden alle ein- und ausgehenden Daten akzeptiert.

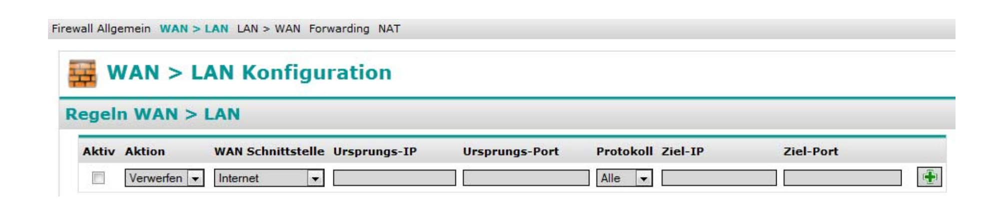
!

Die Auswahl „Minimalste Sicherheitsstufe“ sollte nur zu Testzwecken kurzzeitig eingestellt werden, da jeglicher Datenverkehr und Zugriff von außen möglich ist!

Der Punkt „Alle Absender IP-Adressen aller ausgehenden LAN-Pakete mit der eigenen LAN-IP-Adresse des Routers ersetzen (SNAT)“ bewirkt, dass die LAN-IP des REX 300 nicht als Gateway eingestellt werden muss.

10.2 Sicherheitseinstellungen – WAN>LAN

Über diese Einstellung wird der eingehende Datenverkehr geregelt, d. h., die nachfolgend aufgeführten Einstellungen gelten nur für den von außen eingehenden Datenverkehr.

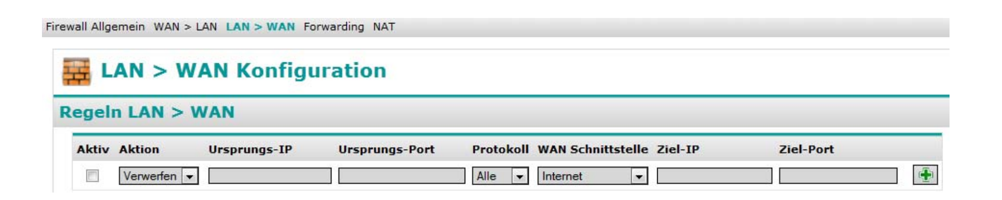


Bezeichnung	Funktion/Beschreibung
Aktiv	Versehen Sie die Checkbox durch einen Mausklick mit einem Haken, damit die nachfolgenden Einstellungen nach dem Speichern aktiv sind.
Aktion	Folgende Optionen stehen zur Auswahl:
	Verwerfen: Wird diese Option gewählt, dann dürfen keine Datenpakete passieren. Der Absender erhält hierbei keine Information über deren Verbleib.
	Abweisen: Bei dieser Option werden die Datenpakete zurückgewiesen. Der Absender erhält eine Information darüber, dass die Datenpakete zurückgewiesen wurden.
	Akzeptieren: Hier dürfen die Datenpakete passieren.
WAN Schnittstelle	Hier kann explizit die gewünschte Schnittstelle für die Firewallregel ausgewählt werden. Will man z. B. den Datenverkehr von WAN Ethernet nach LAN erlauben, dann muss „Akzeptieren“ und „WAN Ethernet“ eingetragen werden.
Ursprungs-IP	Tragen Sie hier die IP ein, für deren eingehende Datenpakete eine der eingestellten Aktionen ausgeführt werden soll. Lässt man das Feld frei, gilt die eingestellte Aktion für alle IP-Adressen.

Ursprungs-Port	Tragen Sie hier den Port ein, über den die Datenpakete eingehen.
Protokoll	Folgende Möglichkeiten stehen zur Auswahl:
	Alle: Die eingestellte Regel gilt für alle Protokolle.
	TCP: Die eingestellte Regel gilt nur für das TCP-Protokoll.
	UDP: Die eingestellte Regel gilt nur für das UDP-Protokoll.
	ICMP: Die eingestellte Regel gilt nur für das ICMP-Protokoll.
Ziel-IP	Tragen Sie hier die IP ein, an die die Datenpakete weitergeleitet werden sollen.
Ziel-Port	Tragen Sie den Port ein, über den die Datenpakete weitergeleitet werden.
	Editieren der Einstellungen in der aktuellen Zeile
	Eingaben in der momentanen Zeile löschen.
	Hiermit werden die eingegebenen Werte als Regel angelegt.
	Temporäres Speichern der angelegten Regel.
	Ändert die Reihenfolge der zuvor angelegten Regel.

10.3 Sicherheitseinstellungen – LAN/WAN

Über diese Einstellung wird der ausgehende Datenverkehr geregelt, d. h., die nachfolgend aufgeführten Einstellungen gelten nur für den von außen eingehenden Datenverkehr.



Bezeichnung	Funktion/Beschreibung
Aktiv	Versehen Sie die Checkbox durch einen Mausklick mit einem Haken, damit die nachfolgenden Einstellungen nach dem Speichern aktiv sind.
Aktion	Folgende Optionen stehen zur Auswahl:
	Verwerfen: Wird diese Option gewählt, dann dürfen keine Datenpakete passieren. Der Absender erhält hierbei keine Information über deren Verbleib.
	Abweisen: Bei dieser Option werden die Datenpakete zurückgewiesen. Der Absender erhält eine Information darüber, dass die Datenpakete zurückgewiesen wurden.
	Akzeptieren: Hier dürfen die Datenpakete passieren.
Ursprungs-IP	Hier wird die IP-Adresse eines Rechners eingetragen von dem aus Datenpakete ins Internet geschickt werden dürfen. Lässt man das Feld frei, gilt die eingestellt Aktion für alle IP-Adressen
Ursprungs-Port	Hier wird der Port eingetragen, über den die Datenpakete ins Internet gesendet werden.

Protokoll	Folgende Möglichkeiten stehen zur Auswahl:
	Alle: Die eingestellte Regel gilt für alle Protokolle.
	TCP: Die eingestellte Regel gilt nur für das TCP-Protokoll.
	UDP: Die eingestellte Regel gilt nur für das UDP-Protokoll.
	ICMP: Die eingestellte Regel gilt nur für das ICMP-Protokoll.
Ziel-IP	Tragen Sie hier die Zieladresse der Datenpakete im Internet ein.
Ziel-Port	Tragen Sie hier den Port ein, über den die Datenpakete zur Ziel-IP geschickt werden.
	Editieren der Einstellungen in der aktuellen Zeile.
	Eingaben in der momentanen Zeile löschen.
	Hiermit werden die eingegebenen Werte als Regel angelegt.
	Temporäres Speichern der angelegten Regel.
	Ändert die Reihenfolge der zuvor angelegten Regel.

10.4 Sicherheitseinstellungen – Forwarding

Über diese Einstellung werden Anfragen von bestimmten IP-Adressen und Ports wiederum an definierte IP-Adressen und Ports weitergeleitet.

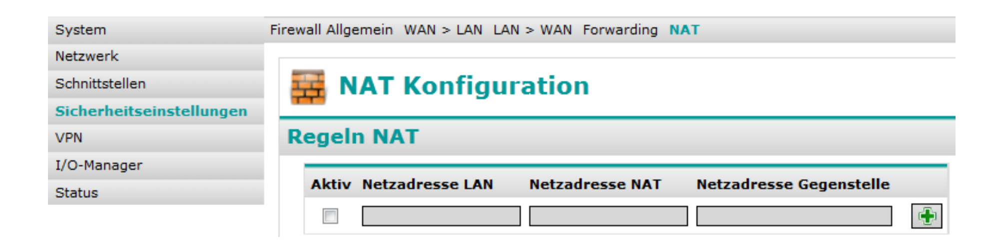


Bezeichnung	Funktion/Beschreibung
Aktiv	Versehen Sie die Checkbox durch einen Mausklick mit einem Haken, damit die nachfolgenden Einstellungen nach dem Speichern aktiv sind.
Ursprungs-IP	Hier können Sie die IP-Adresse eintragen, von der die Datenpakete empfangen werden. Wird hier ein Eintrag vorgenommen, werden nur Pakete von dieser einen Adresse weitergeleitet.
Ursprungs-Port	Hier können Sie den Port eintragen, über den die Datenpakete eingehen. Wird hier ein Eintrag vorgenommen, dann werden nur Pakete die speziell über diesen Port geschickt werden weitergeleitet.
Protokoll	Folgende Protokolle stehen zur Auswahl:
	Alle: Die eingestellte Regel gilt für alle Protokolle.
	TCP: Die eingestellte Regel gilt nur für das TCP-Protokoll.
	UDP Die eingestellte Regel gilt nur für das UDP-Protokoll.
Ziel-IP	Hier die IP-Adresse eintragen, an die die Datenpakete ursprünglich gesendet werden sollten.
Ziel-Port	Hier den Port angeben, über den die Datenpakete ursprünglich zur Ziel-IP gesendet werden sollten.
an IP weiterleiten	Hier die IP-Adresse eintragen, an die die Datenpakete tatsächlich weitergeleitet werden sollen.

an Port weiterleiten	Hier den Port angeben, über den die Datenpakete tatsächlich weitergeleitet werden sollen.
Auf alle Verbindungen anwenden	Der "FORWARDING"-Eintrag wird auf alle Verbindungen angewendet. D.h. auch eingehende VPN-Verbindungen. Ohne diese Option gilt der Eintrag nur für eingehende Pakete aus dem Internet, nicht jedoch eine VPN-Verbindung über das Internet.
	Editieren der Einstellungen in der aktuellen Zeile.
	Eingaben in der momentanen Zeile löschen.
	Hiermit werden die eingegebenen Werte als Regel angelegt.
	Temporäres Speichern der angelegten Regel.
	Ändert die Reihenfolge der zuvor angelegten Regel.

10.5 Sicherheitseinstellungen – NAT

Über diese Einstellung ist es möglich zwei Netzwerke, die im gleichen Adressbereich liegen, trotzdem miteinander zu verbinden. Wenn zum Beispiel ein Netzwerk mit der Netzadresse 192.168.0.0/24 mit einem Netzwerk der gleichen Netzadresse verbunden werden soll, so ist das nur möglich, wenn einem der beiden Netze eine andere Adresse zugewiesen wird. Mithilfe der NAT-Technik (Network Address Translation) ist dies auf einfache Weise zu realisieren, da hier lediglich die eigentliche Netzadresse (Netzadresse LAN) und die Ersatzadresse (Netzadresse NAT) benötigt werden. Der NAT-Algorithmus sorgt dann dafür, dass ausschließlich für die Kommunikation dieser beiden Netze die Adressen in den Datenpaketen entsprechend ersetzt werden. Somit muss die eigene Netzadressierung nicht angepasst werden.



Bezeichnung	Funktion/Beschreibung
Aktiv	Versehen Sie die Checkbox durch einen Mausklick mit einem Haken, damit die nachfolgenden Einstellungen nach dem Speichern aktiv sind.
Netzadresse LAN	Geben Sie hier die reelle Netzadresse des Netzwerkes (z. B. 192.168.0.0/24) ein. Bitte beachten Sie, dass die Netzadresse in CIDR-Schreibweise eingetragen werden muss.
Netzadresse NAT	Geben Sie hier die umgesetzte Adresse Ihres Netzwerkes an (z. B. 192.168.1.0/24). Bitte beachten Sie, dass die Netzadresse in CIDR-Schreibweise eingetragen werden muss.
Netzadresse Gegenstelle	Geben Sie hier die Adresse des Netzwerkes an, zu dem die umgesetzten Pakete geroutet werden sollen. Falls die Gegenstelle auch eine Adressumsetzung verwendet, muss hier die NAT-Adresse der Gegenstelle eingetragen werden.
	Hiermit werden die eingegebenen Werte als Regel angelegt.

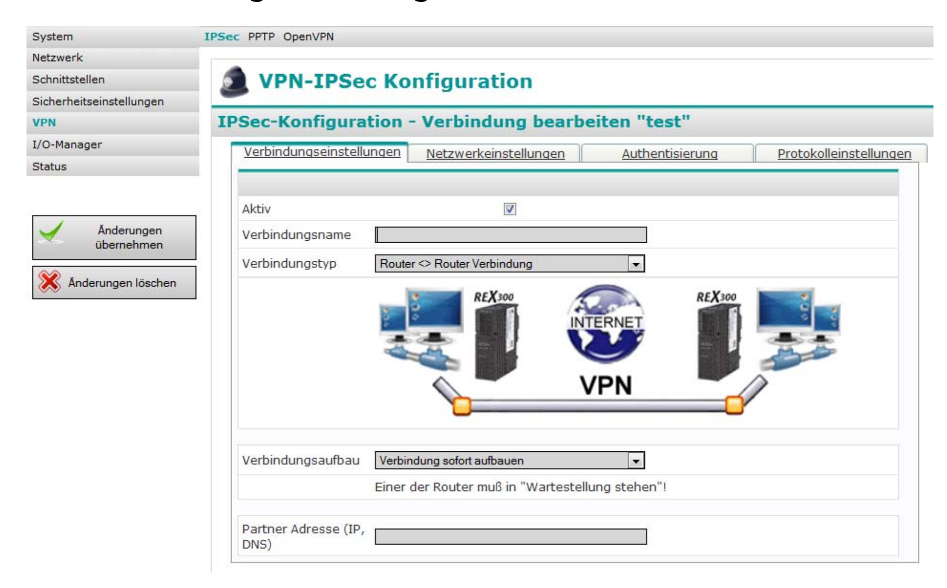
11 VPN

11.1 VPN – IPSec

11.1.1 Verbindungseinstellungen



Bitte beachten Sie, dass grundsätzlich IPSec- und PPTP-VPN Verbindungen nur mit einem REX 300 mit zusätzlicher WAN Schnittstelle möglich sind.

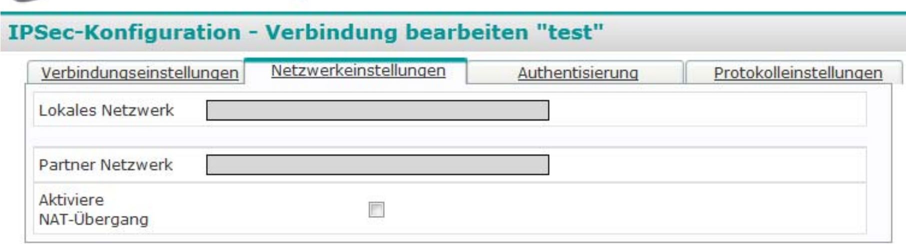


Bezeichnung	Funktion/Beschreibung
Aktiv	Versehen Sie die Checkbox durch einen Mausklick mit einem Haken, damit die nachfolgende VPN-Verbindung samt Einstellungen nach dem Speichern aktiv ist.
Verbindungsname	Tragen Sie in das Eingabefeld einen Namen für die Verbindung ein.
Verbindungstyp	Wählen Sie über das Auswahlfeld den Verbindungstyp: *Router <> Router Verbindung* oder *Client <> Router Verbindung*
Verbindungsaufbau (nur bei Router-Router-Verbindung)	Bitte beachten Sie, dass zur Kommunikation mit einem anderen Router dieser für den Zugang ins Internet und auf Anfragen von Clients entsprechend konfiguriert sein muss. Bei einer Router zu Router-Verbindung ist unter folgenden Möglichkeiten des Verbindungsaufbaus auszuwählen:
	Verbindung sofort aufbauen: Nach einem Neustart bzw. Bootvorgang wird eine Verbindung aufgebaut.
	Verbindung bei Datenverkehr aufbauen: Die Verbindung zum Router bzw. gege-

	nüberliegenden Netzwerk erfolgt bei Anfragen aus dem lokalen Netzwerk.
	Warten auf eingehende Verbindung: Der Router, der sich in Wartestellung befindet, ist der sog. VPN-Server. Er wartet auf eingehende Verbindungen.
Partner Adresse (IP, DNS) (nur bei Router-Router-Verbindung)	Beim Router, der für die ausgehenden Verbindung zuständig ist, muss die entsprechende Partneradresse angegeben werden. Dies kann eine IP-Adresse oder auch der DNS-Name sein, unter dem der gegenüberliegende Router erreichbar ist.

11.1.2 Netzwerkeinstellungen

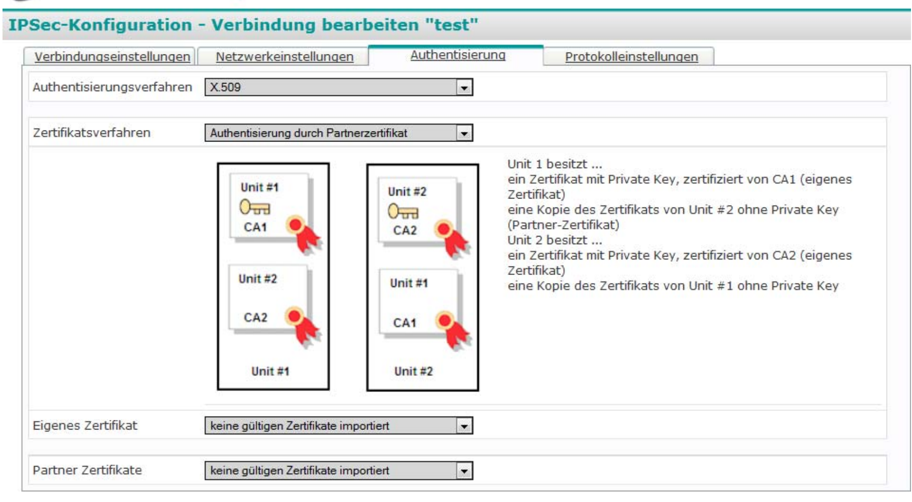




Bezeichnung	Funktion/Beschreibung
Lokales Netzwerk	Geben Sie hier den Adressbereich des lokalen Netzwerkes in der CIDR-Schreibweise ein. (z. B. 192.168.0.0/24)
Partner Netzwerk (nur bei Router-Router-Verbindung)	Geben Sie hier den Adressbereich des Partner Netzwerkes in der CIDR-Schreibweise ein. (z. B. 192.168.10.0/24)
Aktiviere NAT-Übergang (nur bei Router-Router-Verbindung)	Diese Einstellung wird benötigt, wenn die VPN-Verbindung über das Internet aufgebaut wird und zwischen dem LAN und dem WAN „genattet“ wird (NAT: Network Address Translation) Diese Einstellung ist in der Regel aktiviert.
Erlaubtes Netzwerk für den Client: (nur bei Client-Router-Verbindung)	Stellen Sie hier ein, auf welches Netzwerk der Client zugreifen darf. Die Eingabe erfolgt in der CIDR-Schreibweise.
Client hat feste IP-Adresse oder Namen (nur bei Client-Router-Verbindung)	Falls der Client eine feste statische IP-Adresse besitzt, dann ist die Adresse im nachfolgenden Eingabefeld einzutragen.
Win2000/XP Client (L2TP): (nur bei Client-Router-Verbindung)	Stellen Sie ein, ob es sich beim Client um einen PC mit Betriebssystem Windows 2000 oder Windows XP handelt.

11.1.3 Authentisierung





Bezeichnung	Funktion/Beschreibung
Authentisierungsverfahren	Wählen Sie über dieses Auswahlfeld das Authentisierungsverfahren aus.
	PSK: Beide Schlüssel müssen vor dem Datenaustausch zwischen Client und Router bekannt sein. Umso länger der Schlüssel ist, desto sicherer ist die Verbindung. Es kann nur ein Schlüssel angegeben werden. Auch wenn mehrere PSK-Verbindungen eingetragen werden, gilt für diese nur der Schlüssel der ERSTEN Verbindung. **Lokale ID:** Vergeben Sie hier einen Namen für Ihren Router. Dieser Name muss dem Partner mitgeteilt werden. **Partner ID:** Tragen Sie hier den Namen des Partners ein.

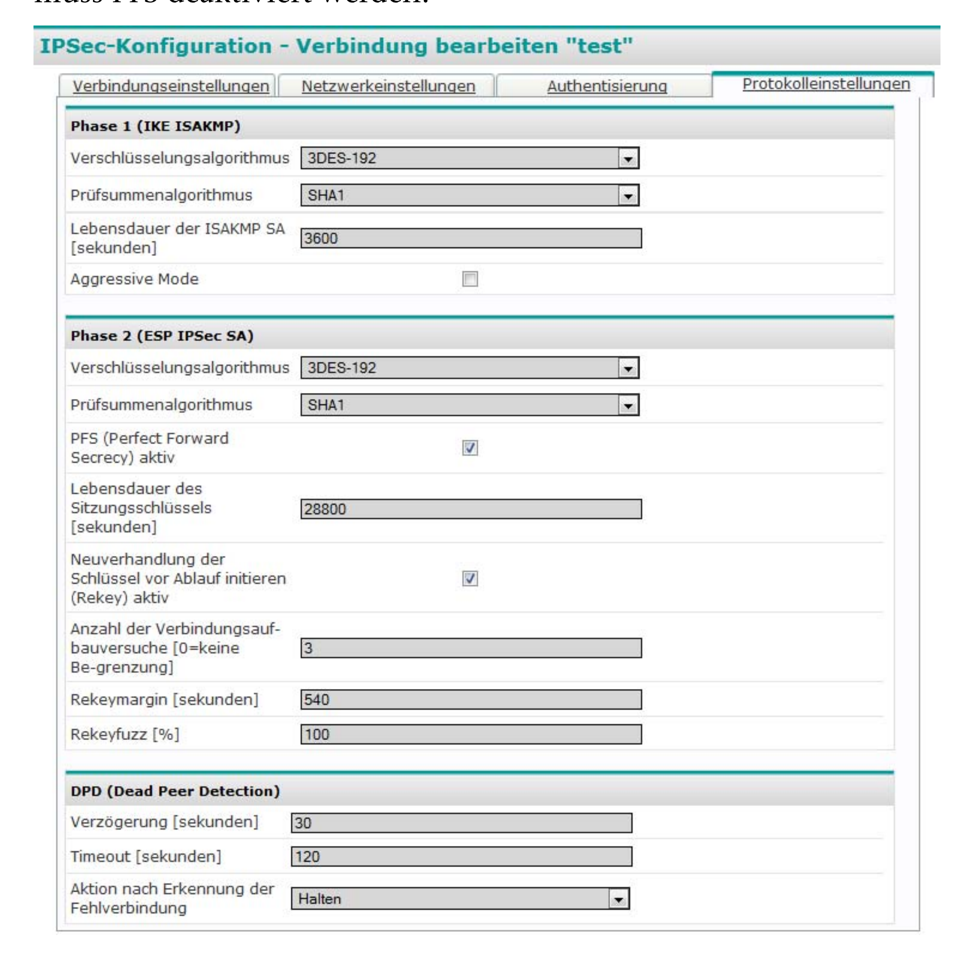
Authentisierungsverfahren (Fortsetzung)	**X.509:** Hierbei können Sie über das Feld aus zwei Zertifikatsverfahren auswählen: **Authentisierungsverfahren durch eine CA:** Hierzu muss auf dem Router das Stammzertifikat (Unterzeichnende Stelle, kurz CA) und das eigene Zertifikat inklusive Schlüssel (.p12-Datei) importiert sein. (Siehe Kapitel System – Zertifikate) Die Gegenstelle muss dasselbe Stammzertifikat und ein von der CA unterzeichnetes Zertifikat inklusive Schlüssel besitzen. **Authentisierung durch Partnerzertifikate:** Hierbei können die Zertifikate von unterschiedlichen CAs unterzeichnet sein. Auf jedem Router muss ein eigenes Zertifikat+Schlüssel (.p12-Datei) importiert sein. Ebenso eine Kopie des jeweiligen Partnerzertifikates, natürlich OHNE Schlüssel (.crt-Datei) **Eigenes Zertifikat:** Wählen Sie das eigene Zertifikat über die Auswahlfläche aus. **Lokale ID:** Diese ID wird normalerweise vom Zertifikat bestimmt. Dieses Feld kann leer gelassen werden.

Authentisierungsverfahren (Fortsetzung)	**Partner Zertifikat:** Wählen Sie das Zertifikat des Partners aus. **Partner ID:** Diese ID kann nur vom Zertifikat bestimmt werden, wenn man *„Authentisierungsverfahren durch Partnerzertifikate"* gewählt hat. In diesem Fall kann das Feld leer gelassen werden. Hat man sich jedoch für das *„Authentisierungsverfahren durch eine CA„* entschieden, so muss man – nur für den Fall, dass man die Verbindung aufbaut – die ID des Partners angeben. Diese ID wird beim Erstellen des Zertifikats ausgewählt. Es handelt sich um das sogenannte Subject des Zertifikats und muss in folgender Art und Weise eingetragen werden: /C=land/ST=bundesland/L=stadt /O=firma/OU=abteilung/CN=name_ zertifkat/E=emailadresse Wenn bei der Erstellung des Zertifikates nicht alle Felder unter der Registerkarte Subject ausgefüllt werden, so sind die entsprechenden Einträge wegzulassen. **Partner Zertifikate:** Nur bei Auswahl *„Authentisierung durch Partnerzertifikate"*. Auswahl des entsprechenden Zertifikates über das Auswahlfeld.

11.1.4 Protokolleinstellungen

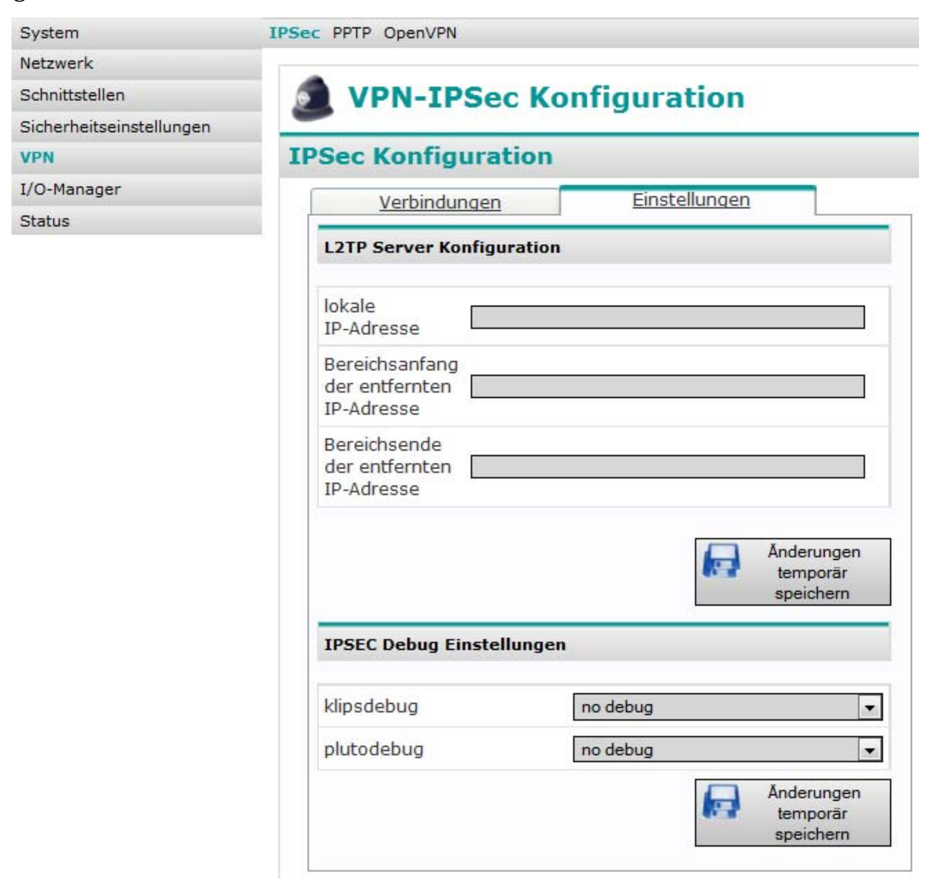
Wählen Sie in diesem Menü die während der verschiedenen Phasen stattfindenden Verschlüsselungsalgorithmen, Prüfsummenbildung usw. aus.

Die Einstellung PFS ist nur für die Router-Router-Verbindung erlaubt. Falls Sie eine Client-Router-Verbindung einrichten möchten, muss PFS deaktiviert werden.



11.1.5 L2TP Server Konfiguration

Für die VPN-IPSec-Kommunikation zwischen dem Industrierouter und einem Windowsclient ist es möglich, den L2TP-Server zu verwenden. Hier ist lediglich eine frei wählbare lokale IP-Adresse einzustellen. Aus dem gleichen Netz sollten dann die Adressen für die Clients eingestellt sein, deren Bereichsanfang und –ende weiter unten eingestellt werden kann. Der L2TP-Server funktioniert dann ähnlich wie ein DHCP-Server und kann die Adressen aus dem eingestellten Bereich an sich einwählende Clients automatisch vergeben.



Bezeichnung	Funktion/Beschreibung
Lokale IP-Adresse	Hier ist der Name oder die IP-Adresse einzutragen, die der Server während der Kommunikation mit dem Windows-Client haben soll. (z. B. 192.168.0.110)
Bereichsanfang der entfernten IP-Adresse	Vergabe der IP-Adressen an Clients. Hier kann der Adressbereich eingestellt werden, aus welchem entfernte Clients ihre IP zugeteilt bekommen. (z. B. 192.168.0.130 bis 192.168.0.140)
Bereichsende der entfernten IP-Adresse	

11.2 VPN – PPTP

11.2.1 Server



Bitte beachten Sie, dass grundsätzlich IPSec- und PPTP-VPN Verbindungen nur mit einem REX 300 mit zusätzlicher WAN Schnittstelle möglich sind.

Helmholz
COMPATIBLE WITH YOU

System
Netzwerk
Schnittstellen
Sicherheitseinstellungen
VPN
I/O-Manager
Status

IPSec PPTP OpenVPN

VPN-PPTP Konfiguration

PPTP Konfiguration

Server Clients

Server Konfiguration
Aktiv

automatische Konfiguration: nein

lokale IP-Adresse oder Bereich
entfernte IP-Adresse oder Bereich
DNS-Server IP-Adresse an Client
WINS-Server IP-Adresse an Client

Verschlüsselung Konfiguration
Verschlüsselung: MPPE V2 Alle

Authentisierung Konfiguration
Authentifizierung via PAP
Authentifizierung via CHAP
Authentifizierung via MS-CHAP
Authentifizierung via MS-CHAP V2

Änderungen temporär speichern

Bezeichnung	Funktion/Beschreibung
Aktiv	Soll der Industrierouter als PPTP-VPN-Server aktiviert werden, dann ist die Checkbox mit einem Haken zu versehen.

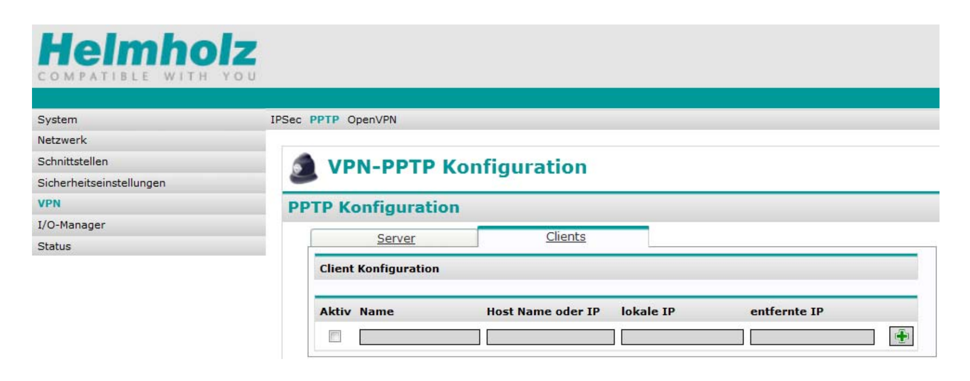
<table>
<tr><td>Automatische Konfiguration</td><td>Wenn Sie hier „ja“ auswählen, dann wird die lokale Adresse des REX 300 verwendet. Sollten Sie „Nein“ ausgewählt haben, dann beachten Sie Folgendes.</td></tr>
<tr><td>Lokale IP Adresse oder Bereich</td><td rowspan="2">Für den Aufbau eines Übertragungskanals ist eine lokale und eine entfernte Adresse (Anfangs- und Endpunkt des VPN-Tunnels) notwendig. Sie haben hier die Möglichkeit, entweder eine einzelne IP-Adresse oder einen ganzen Bereich einzugeben. Bei der Angabe des entfernten Bereichs bestimmt dieser die maximale Anzahl der sich gleichzeitig einwählenden Clients.

Beispiel:
Lokale IP-Adresse: 192.168.0.104
Entfernte IP-Adresse:192.168.0.160
Der VPN-Server ist unter der IP-Adresse 192.168.0.104 erreichbar. Es kann sich nur ein einzelner Client, dem die IP-Adresse 192.168.0.160 (vom Server) zugewiesen wird, am Server anmelden.

Beispiel:
Lokale IP-Adresse: 192.168.0.104
Entfernte IP-Adresse:192.168.0.160-170
Den angeschlossenen Clients (max. 10), die sich gleichzeitig einwählen dürfen, werden vom Server 192.168.0.104 die IP-Adressen 192.168.0.160 bis 192.168.0.170 zugewiesen.</td></tr>
<tr><td>Entfernte IP-Adresse oder Bereich</td></tr>
<tr><td>DNS-Server IP-Adresse an Client</td><td>Geben Sie hier die DNS-Server-Adresse ein, die einem auf dem Router eingewählten Client zugeordnet wird, um Rechnernamen in IP-Adresse und umgekehrt aufzulösen.</td></tr>
<tr><td>WINS IP-Adresse an Client</td><td>Tragen Sie hier die WINS-Server-Adresse für die NetBIOS-Namensauflösung ein, die einem auf dem Router eingewählten Client zugeordnet wird.</td></tr>
</table>

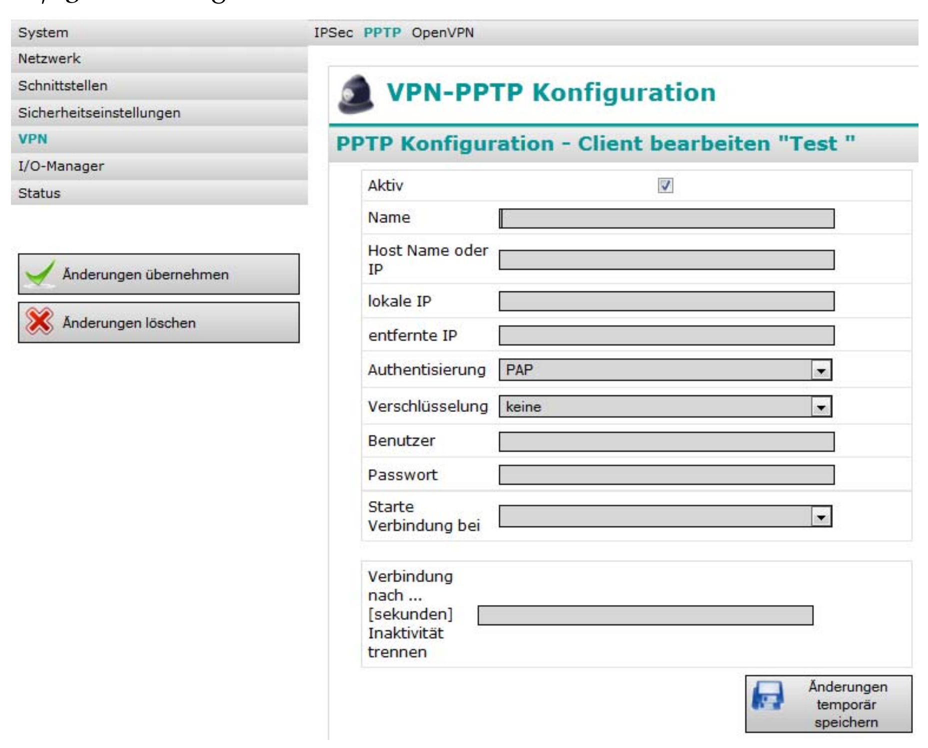
Verschlüsselung	Wählen Sie hier die entsprechende Verschlüsselungsart über das Auswahlfeld:
	Keine: Keine Verschlüsselung.
	MPPE V2 40: 40-Bit-Verschlüsselung.
	MPPE V2 128: 128-Bit-Verschlüsselung.
	MPPE V2 Alle: Alle Verschlüsselungen.
Authentifizierung via PAP	Wenn Sie diese Art der Authentifizierung wählen, schickt der Client dem Host die Benutzername/Passwort-Kombination so lange, bis der Host die Authentifizierung des Clients annimmt oder ablehnt.
Authentifizierung via CHAP	Wenn Sie diese Art der Authentifizierung wählen, wird die Authentifizierung vom Host gesteuert. Hat sich ein Client eingewählt, dann wird er vom Host zur Authentifizierung aufgefordert. Die Kombination aus Benutzername und Passwort wird dann vom Client per MD5 Algorithmus verschlüsselt übertragen. Stimmen die gesendeten Benutzerdaten mit denen des Hosts überein, dann wird die Authentifizierung akzeptiert. Wenn nicht, wird sie abgelehnt. Wenn die Authentifizierung akzeptiert wird, werden während der Verbindung die Benutzerdaten periodisch überprüft.
Authentifizierung via MS-CHAP	Von Microsoft eigens entwickeltes Authentifizierungsprotokoll.
Authentifizierung via MS-CHAP V2	Von Microsoft eigens entwickeltes Authentifizierungsprotokoll.

11.2.2 Client



Bezeichnung	Funktion/Beschreibung
Aktiv	Soll der Industrierouter als PPTP-VPN-Client betrieben werden, dann ist die Checkbox mit einem Haken zu versehen.
Name	Tragen Sie hier einen Namen für den Client ein.
Host Name oder IP	Tragen Sie hier den Namen oder die IP-Adresse ein, unter der der Client den Server erreicht. Beispiel R00007805.REX300.my-rex.net oder 80.147.33.44
Lokale IP	Diese Eingabe ist optional. Wenn der Server nicht so konfiguriert ist, dass er dem Client eine IP-Adresse zuteilt, dann kann der Client hiermit diese eingetragene IP-Adresse verlangen. In der Regel werden die Einstellungen am VPN-Server durchgeführt. Die Einstellmöglichkeit dient hier der Kompatibilität mit anderen Routern.
Entfernte IP	Tragen Sie hier die Netzadresse des Servers in CIDR-Schreibweise ein (Bsp. 192.168.0.0/24), um eine Route in das Servernetz zu haben.

Nun folgen die Einstellungen, nachdem Sie die Schaltfläche „*Hinzufügen*“ betätigt haben.



Bezeichnung	Funktion/Beschreibung
Aktiv	Soll der Industrierouter als PPTP-VPN-Client betrieben werden, dann ist die Checkbox mit einem Haken zu versehen.
Name	Tragen Sie hier einen Namen für den Client ein.
Host Name oder IP	Tragen Sie hier den Namen oder die IP-Adresse ein, unter der der Client den Server erreicht. Beispiel R00007805.REX300.my-rex.net oder 80.147.33.44
Lokale IP	Diese Eingabe ist optional. Wenn der Server nicht so konfiguriert ist, dass er dem Client eine IP-Adresse zuteilt, dann kann der Client hiermit diese eingetragene IP-Adresse verlangen. In der Regel werden die Einstellungen am VPN-Server durchgeführt. Die Einstellmöglichkeit dient hier der Kompatibilität mit anderen Routern.

Entfernte IP	Tragen Sie hier die Netzadresse des Servers in CIDR-Schreibweise ein (Bsp. 192.168.0.0/24) um eine Route in das Servernetz zu konfigurieren.
Authentisierung	Wählen Sie hier die entsprechende Authentifizierungsmethode über das Auswahlfeld:
	PAP: Wenn Sie diese Art der Authentifizierung wählen, schickt der Client dem Host die Benutzername/Passwort-Kombination so lange, bis der Host die Authentifizierung des Clients annimmt oder ablehnt.
	CHAP: Wenn Sie diese Art der Authentifizierung wählen, wird die Authentifizierung vom Host gesteuert. Hat sich ein Client eingewählt, dann wird er vom Host zur Authentifizierung aufgefordert. Die Kombination aus Benutzername und Passwort wird dann vom Client per MD5 Algorithmus verschlüsselt übertragen. Stimmen die gesendeten Benutzerdaten mit denen des Hosts überein, dann wird die Authentifizierung akzeptiert. Wenn nicht, wird sie abgelehnt. Wenn die Authentifizierung akzeptiert wird, werden während der Verbindung die Benutzerdaten periodisch überprüft.
	MSCHAP: Von Microsoft eigens entwickeltes Authentifizierungsprotokoll.
	MSCHAP V2: Von Microsoft eigens entwickeltes Authentifizierungsprotokoll.
Verschlüsselung	Wählen Sie hier die entsprechende Verschlüsselungsart über das Auswahlfeld:
	Keine: Keine Verschlüsselung.
	MPPE V2 40: 40-Bit-Verschlüsselung.
	MPPE V2 128: 128-Bit-Verschlüsselung.
	MPPE V2 Alle: Alle MPPE Verschlüsselungen.

Benutzer	Geben Sie hier den Benutzernamen für Ihren PPTP-Server ein.
Passwort	Geben Sie hier das zum Benutzer zugehörige Passwort Ihres PPTP-Servers ein.
Starte Verbindung bei	Wählen Sie mit diesem Auswahlfeld aus, wann die VPN-Verbindung initiiert werden soll. Die folgenden Optionen stehen zur Verfügung:
	Verbindung immer aufrechterhalten: Die Verbindung wird aufgebaut, sobald das Gerät gestartet wird.
	Verbindung bei Datentransfer: Die Verbindung zum Router bzw. gegenüberliegenden Netzwerk erfolgt bei Anfragen aus dem lokalen Netzwerk.
	Starten bei aktiver Internetverbindung: Die Verbindung wird aufgebaut, nachdem eine Internetverbindung über das interne oder ein externes Modem hergestellt wurde.
Verbindung nach … [sekunden] Inaktivität trennen	Hiermit stellen Sie ein, nach welcher Zeit die bestehende VPN-Verbindung getrennt werden soll, sobald keine Datenpakete mehr vom Router versandt werden. Wenn Sie das Feld leer lassen, ist diese Funktion deaktiviert.

11.3 VPN – OpenVPN

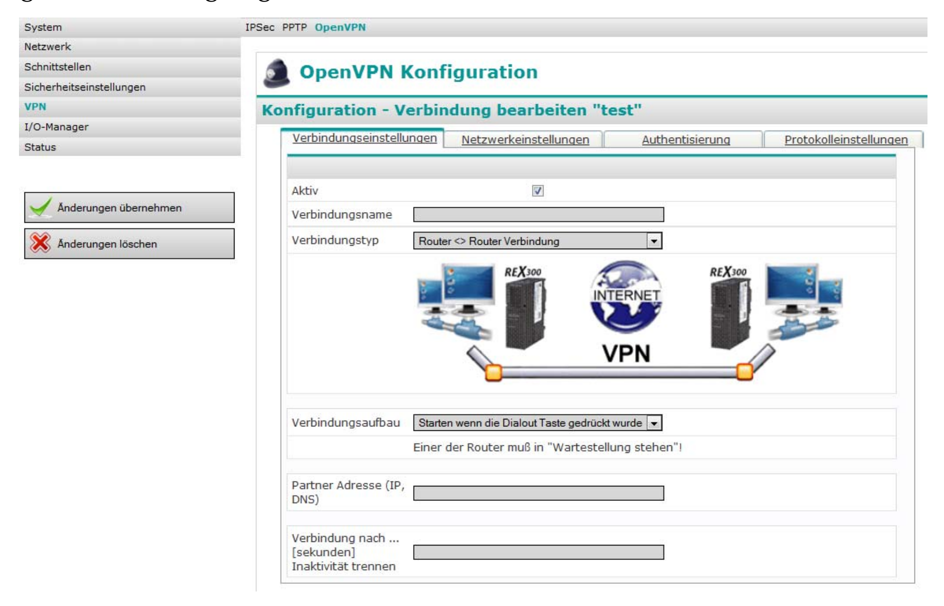
11.3.1 Allgemeines

Folgende Punkte sollten Sie beachten:

- OpenVPN arbeitet grundsätzlich mit zwei Tunnel-IP-Adressen. D. h., jede Verbindung hat zwei IP-Adressen, über die der Datenverkehr abgewickelt wird.
- Abhängig von der Authentifizierungsmethode arbeitet OpenVPN entweder im Punkt-zu-Punkt-Verfahren (bei statischem Schlüssel oder keiner Authentifizierung) oder im Server/Clientmodus (mit X.509 Zertifikaten).
- OpenVPN beherrscht drei verschiedene Authentifizierungsmethoden:
    - keine
      (Es ist kein Zertifikat oder Schlüssel notwendig)
      Dient hauptsächlich zum Testen der Verbindung.
      Die Tunneldaten werden ebenfalls NICHT verschlüsselt.
    - statischer Schlüssel
      Für die Verbindung wird ein 1024-Bit-Schlüssel generiert, den jeder Partner benötigt. Ähnlich einem Passwort.
    - X.509 Zertifikate
      Bei Zertifikaten werden folgende Varianten unterschieden:
        - Jeder Teilnehmer benötigt dasselbe RootCA und ein von der RootCA unterzeichnetes eigenes Zertifikat.
        - Wie der 1. Punkt, jedoch mit zusätzlicher Benutzer- und Passwortabfrage.
        - Wie der 2. Punkt, jedoch ohne eigenes Zertifikat. D. h., die Teilnehmer benötigen nur ein RootCA, Benutzername und Passwort.
- OpenVPN kann einen HTTP-Proxyserver als ausgehende Verbindung benutzen. Wichtig bei der Integration in bestehende Firmennetzwerke mit Internetschluss.
- Die Einstellung des Übertragungsprotokolls (UDP oder TCP) ist bei OpenVPN frei einstellbar.
- Die verwendeten Portnummern sind bei OpenVPN frei einstellbar.

11.3.2 Verbindungseinstellungen

Nachdem Sie eine Verbindung unter VPN – OpenVPN über den *„Hinzufügen"* Button angelegt haben stehen, folgende Einstellungen zur Verfügung.



Bezeichnung	**Funktion/Beschreibung**
Aktiv	Versehen Sie die Checkbox durch einen Mausklick mit einem Haken, damit die nachfolgende VPN-Verbindung samt Einstellungen nach dem Speichern aktiv ist.
Verbindungsname	Tragen Sie in das Eingabefeld einen Namen für die Verbindung ein
Verbindungstyp	Wählen Sie über das Auswahlfeld den Verbindungstyp: *Router <> Router Verbindung* oder *Client <> Router Verbindung*
Verbindungsaufbau (nur bei Router-Router-Verbindung)	Bitte beachten Sie, dass zur Kommunikation mit einem anderen Router dieser für den Zugang ins Internet und auf Anfragen von Clients entsprechend konfiguriert sein muss. Bei einer Router zu Router-Verbindung ist unter folgenden Möglichkeiten des Verbindungsaufbaus auszuwählen:
Verbindungsaufbau (nur bei Router-Router-Verbindung) (Fortsetzung)	**Verbindung sofort aufbauen:** Nach einem Neustart bzw. Bootvorgang wird eine Verbindung aufgebaut.
	Starten bei aktiver Internetverbindung: Die Verbindung zum Router bzw. gegenüberliegenden Netzwerk erfolgt nach

	der Einwahl in das Internet (z. B. über das integrierte Modem).
	Warten auf eingehende Verbindung: Der Router, der sich in Wartestellung befindet, ist der sog. VPN-Server. Er wartet auf eingehende Verbindungen
	Starten wenn die Dialout Taste gedrückt wurde: Die VPN-Verbindung zur Gegenstelle wird nach betätigen der Dialout Taste, die sich über der MPI/PROFIBUS Schnittstelle befindet, aufgebaut.
Partner Adresse (IP, DNS) (nur bei Router-Router-Verbindung)	Beim Router, der für die ausgehende Verbindung zuständig ist, muss die entsprechende Partneradresse angegeben werden. Dies kann eine IP-Adresse oder auch der DNS-Name sein, unter dem der gegenüberliegende Router erreichbar ist.
Verbindung nach … [sekunden] Inaktivität trennen	Hiermit stellen Sie ein, nach welcher Zeit die bestehende VPN-Verbindung getrennt werden soll, sobald keine Datenpakete mehr vom Router versandt werden. Wenn Sie das Feld leer lassen, ist diese Funktion deaktiviert.

Hinweis!

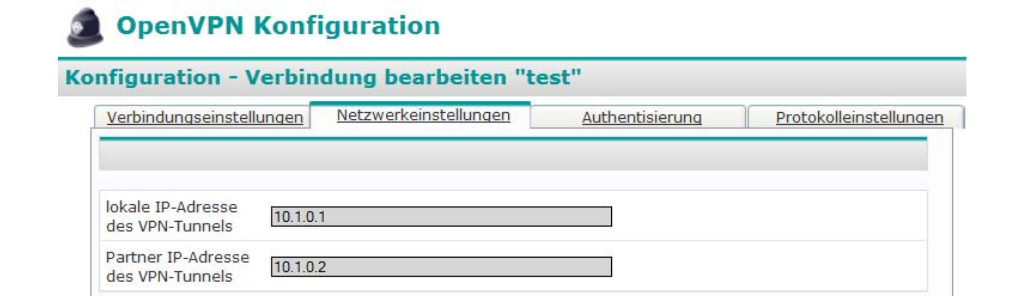
Wurde für den Verbindungsaufbau „*Warten auf eingehende Verbindung*“ gewählt, so ist dieser REX 300 im Servermodus.

Wurde für den Verbindungsaufbau „*Verbindung sofort aufbauen*“ oder „*Starten bei aktiver Internetverbindung*“ gewählt, so ist dieser REX 300 im Clientmodus.

11.3.3 Netzwerkeinstellungen – Servermodus

!

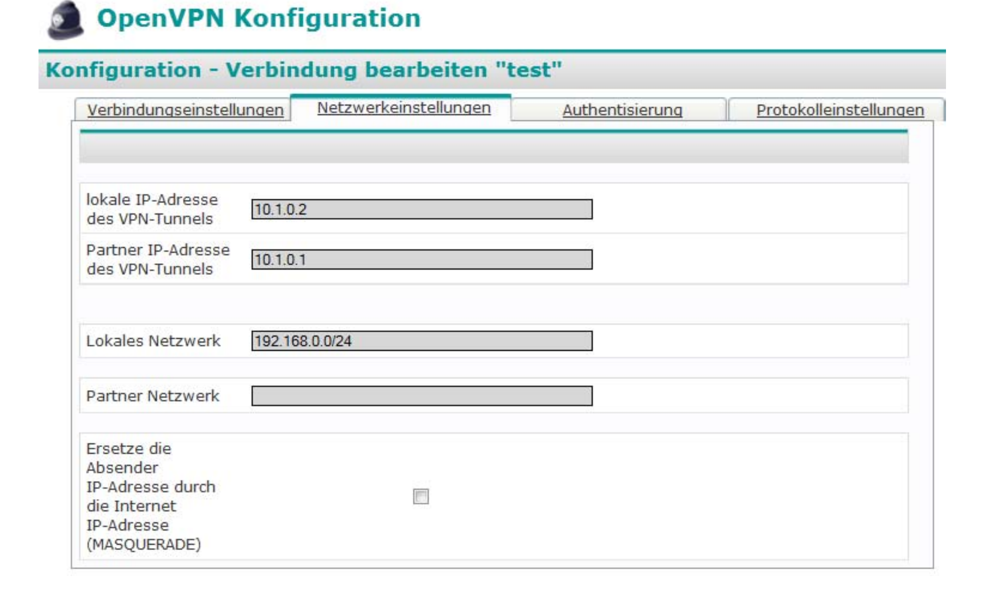
Hier ist der REX 300 im Servermodus und der einwählende PC stellt den Client dar.



Bezeichnung	Funktion/Beschreibung
IP-Adress Bereich für einwählende Clients	Bei der Authentifizierung mit Zertifikaten können sich mehrere Clients am Server anmelden (nicht gleichzeitig) und bekommen automatisch eine IP aus dem *„IP-Adressbereich für einwählende Clients“* zugewiesen. Geben Sie den Adressbereich in der CIDR-Schreibweise ein. (z. B. 10.1.0.1/24)
lokale IP-Adresse des VPN-Tunnels	Geben Sie hier die IP-Adresse des lokalen VPN-Tunnelendpunktes an. (z. B. 10.1.0.1)
Partner IP-Adresse des VPN-Tunnels	Geben Sie hier die IP-Adresse des Partner VPN-Tunnelendpunktes an. (z. B. 10.1.0.1)
Lokales Netzwerk	Tragen Sie hier den Adressbereich des lokalen Netzwerkes in der CIDR-Schreibweise ein. Z. B. 10.1.0.2/24

Es können mehrere Partner mit unterschiedlichen Netzadressen eine VPN-Verbindung aufbauen (nur bei Verwendung von Zertifikaten im Servermodus)	**Nein:** Jeder Client bekommt den Partnernetzwerk-Adressbereich zugewiesen.
	Ja: Bei einer Authentifizierung mit Zertifikaten und diesem Modus, können mehrere Clients gleichzeitig am Server angemeldet sein. Die Clients bekommen dann automatisch aus dem *„IP-Adressbereich für einwählende Clients“* eine Adresse zugewiesen
CN aus Zertifikat oder Benutzername (nur in Kombination mit dem vorherigen Punkt)	Es muss das lokale Netzwerk (oben) und das Partnernetzwerk angegeben werden. In der unteren Liste wird jedem Client ein Netzwerk zugewiesen. Je nach Einstellung in der Authentifizierung (mit Zertifikatsnamen oder Benutzernamen) kann der CN (Common Name im Zertifikat) oder Benutzername ausschlaggebend sein. OpenVPN erstellt je nach gerade einwählendem Client einen entsprechenden Routingeintrag.
Partnernetzwerk (nur wenn die 2 vorherigen Punkte nicht verwendet werden)	Tragen Sie hier den Adressbereich Ihres Partnernetzwerkes in der CIDR-Schreibweise ein. (z. B. 192.168.5.0/24)
Ersetze die Absender IP-Adresse durch die Internet IP-Adresse (MASQUERADE) (nur im Clientmodus)	Diese Option wurde für die Kompatibilität mit mdex eingeführt. Mit dieser Option wird die Absender-IP-Adresse durch die Internet-IP-Adresse ersetzt.

11.3.4 Netzwerkeinstellungen – Clientmodus

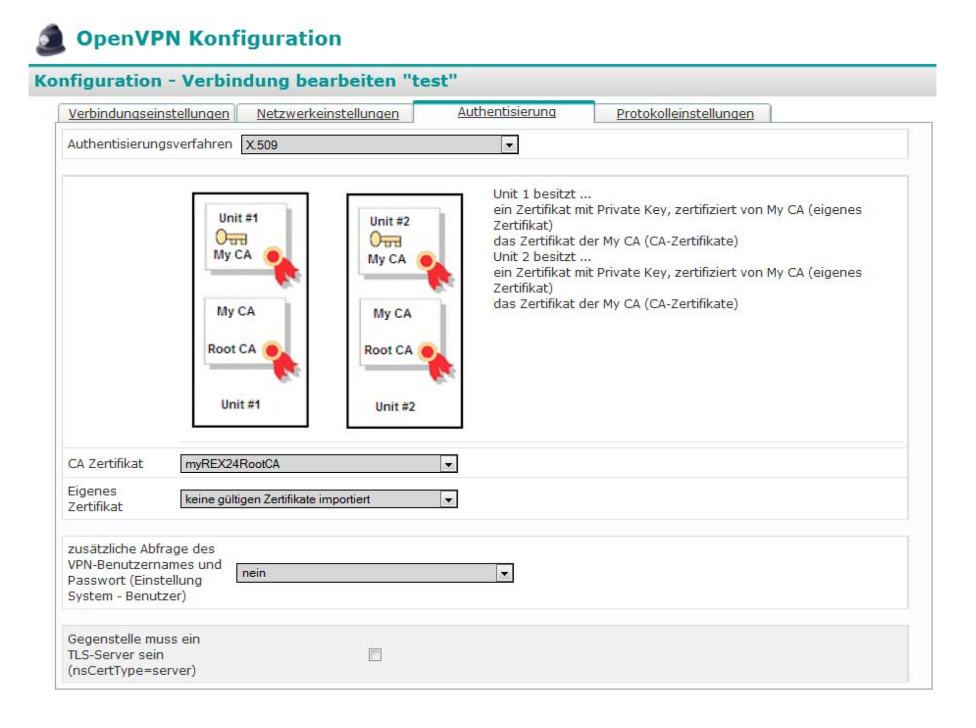


Bezeichnung	Funktion/Beschreibung
IP-Adress Bereich für einwählende Clients	Bei der Authentifizierung mit Zertifikaten können sich mehrere Clients am Server anmelden (nicht gleichzeitig) und bekommen automatisch eine IP aus dem *„IP-Adressbereich für einwählende Clients“* zugewiesen. Geben Sie den Adressbereich in der CIDR-Schreibweise ein. (z. B. 10.1.0.1/24)
lokale IP-Adresse des VPN-Tunnels	Geben Sie hier die IP-Adresse des lokalen VPN-Tunnelendpunktes an. (z. B. 10.1.0.1)
Partner IP-Adresse des VPN-Tunnels	Geben Sie hier die IP-Adresse des Partner VPN-Tunnelendpunktes an. (z. B. 10.1.0.1)
Ersetze die Absender IP-Adresse durch die Internet IP-Adresse (MASQUERADE) (nur im Clientmodus)	Diese Option wurde für die Kompatibilität mit dem Anbieter „mdex“ eingeführt. Mit dieser Option wird die Absender-IP-Adresse durch die Internet-IP-Adresse ersetzt.
Zugriffssteuerung der Clients auf andere Netze: Normalerweise erreichen einwählende Clients nur Netzteilnehmer am LAN des Routers. Hat der Server noch weitere VPN-Verbindungen zu anderen Netzen, so muss im Client die entsprechende Zugriffssteuerung eingetragen werden.	
Der Client hat Zugriff auf folgende Partnernetzwerke (nur bei Authentifizierung mit X.509)	Hier geben Sie die Netzadresse des Partnernetzwerkes an. Z. B. das LAN-Netz des Servers (anderer Router, zudem dieser Router eine VPN-Verbindung aufgebaut hat).
CN aus Zertifikat oder Benutzername	Es muss das lokale Netzwerk (oben) und das Partnernetzwerk angegeben werden. In der unteren Liste wird jedem Client ein Netzwerk zugewiesen. Je nach Einstellung in der Authentifizierung (mit Zertifikatsnamen oder Benutzernamen) kann der CN (Common Name im Zertifikat) oder Benutzername ausschlaggebend sein. OpenVPN erstellt je nach gerade einwählendem Client einen entsprechenden Routingeintrag.
NAT Partnernetzwerk	Ist das andere Netzwerk nur über eine NAT-Adresse erreichbar, so kann hier die Netzwerkadresse optional angegeben werden. Mit dieser Option kann man auch eine sichere Steuerung des NAT-Netzwerkes erreichen.

11.3.5 Authentisierung

OpenVPN bietet drei grundsätzlich unterschiedliche Authentifizierungsarten an.

- keine
  (es ist kein Zertifikat oder Schlüssel notwendig)
  Dient hauptsächlich zum Testen der Verbindung. Die Tunneldaten werden NICHT verschlüsselt.
- statischer Schlüssel
  Für die Verbindung wird ein Schlüssel generiert, den jeder Partner benötigt. Ähnlich einem Passwort.
- X.509 Zertifikate
  Bei Zertifikaten werden drei Varianten unterschieden:
    - o Jeder Teilnehmer benötigt dasselbe RootCA und ein von der RootCA unterzeichnetes eigenes Zertifikat.
    - o Wie der 1. Punkt, jedoch mit zusätzlicher Benutzer- und Passwortabfrage.
    - o Wie der 2. Punkt, jedoch ohne eigenes Zertifikat. D. h., die Teilnehmer benötigen nur ein RootCA, Benutzername und Passwort.



Bezeichnung	Funktion/Beschreibung
Authentisierung-verfahren	Über dieses Auswahlfeld können Sie das Authentisierungsverfahren für Ihre OpenVPN Verbindung einstellen. Folgende Auswahlmöglichkeiten stehen zur Verfügung:
	keine Authentifizierung: Diese Einstellung soll hauptsächlich zu

	Testzwecken dienen. Man kann hiermit sehr schnell und einfach eine Verbindung zu einem Partner testen. In diesem Modus werden die übertragenen Daten unverschlüsselt versendet.
	Authentifizierung mit statischem Schlüssel: Bei der symmetrischen Verschlüsselung erfolgt die Authentifizierung und Verbzw. Entschlüsselung der Daten mit ein und demselben Schlüssel (statischer Schlüssel). Der Vorteil der symmetrischen Verschlüsselung ist die Geschwindigkeit. Das Ver- und Entschlüsseln ist im Gegensatz zur asymmetrischen Verschlüsselung deutlich schneller, da der symmetrische Schlüssel schon ab 90 Bit als sicher gilt – der asymmetrische dagegen sollte mindestens 1024 Bit lang sein. Der Nachteil der symmetrischen Verschlüsselung ist der gegenseitige Schlüsselaustausch. Jeder Teilnehmer muss den Schlüssel auf sichere Art und Weise erhalten.
	X.509 Stellen Sie diesen Menüpunkt ein, wenn Sie das asymmetrische Verschlüsselungsverfahren verwenden möchten. Der Vorteil von Zertifikaten liegt in der Erweiterung des Funktionsumfanges von OpenVPN. Z. B. können mehrere VPN-Clients mithilfe von Zertifikaten parallele Verbindungen zu einem OpenVPN-Server aufbauen.
Statischer Schlüssel (nur bei Authentisierungsverfahren „Statischer Schlüssel“)	Hier kann ein zuvor importierter oder generierter Schlüssel für das Authentifizierungsverfahren *„Statischer Schlüssel“* ausgewählt werden.

CA Zertifikat	Dies ist das Stammzertifikat (RootCA). Von diesem Zertifikat müssen alle anderen Zertifikate abstammen. Hier wählen Sie das entsprechende Zertifikat aus. Importieren können Sie diese über den Menüpunkt **System – Zertifikate**.
Eigenes Zertifikat	Mit diesem Zertifikat authentifizieren Sie sich gegenüber Ihrem VPN-Partner. Hier wählen Sie das entsprechende Zertifikat aus. Importieren können Sie diese über den Menüpunkt **System – Zertifikate**.
zusätzliche Abfrage des VPN-Benutzernamens und Passwort (Einstellung System – Benutzer)	Es ist möglich, dass zusätzlich noch Benutzerdaten vom einwählenden Client gefordert werden. Server: Aktivieren Sie diese Option, wenn Sie die Benutzerverwaltung aus dem Menü Ihres REX 300 verwenden wollen. (**System – Benutzer**) Client: Bitte beachten Sie hierbei, dass diese Benutzerdaten im VPN-Server unter **System – Benutzer** eingetragen sein müssen.
Für die Authentifizierung nur das CA-Zertifikat und Benutzer/Passwort verwenden. (nur Client – Router Verbindung)	Mit dieser Option aktivieren Sie die Authentifizierung über das CA-Zertifikat und die Benutzerdaten aus dem Menü **System – Benutzer**.
Benutzer (nur Clientmodus)	Benutzername eines Benutzers aus dem VPN-Server (**System – Benutzer**)
Passwort (nur Clientmodus)	Passwort des Benutzers aus dem VPN-Server (**System – Benutzer**)
Das eigene Zertifikat nicht für die Authentifizierung benutzen. Nur das CA-Zertifikat und Benutzer/Passwort verwenden. (nur Clientmodus)	Mit dieser Option authentifizieren Sie sich nur über das CA-Zertifikat und die Benutzerdaten des VPN-Servers (aus **System – Benutzer** des Servers)

Gegenstelle muss ein TLS-Server sein (nsCertType=server) (nur im Clientmodus)	Dies ist eine zusätzliche Sicherheitsoption und überprüft, ob das Serverzertifikat den Eintrag „Netscape Certificatetype: SSL-Server“ hat. Ist dieser Zusatz im Serverzertifikat nicht vorhanden, wird der Verbindungsaufbau abgebrochen.

11.3.6 Protokolleinstellungen



Konfiguration - Verbindung bearbeiten "test"

Verbindungseinstellungen | Netzwerkeinstellungen | Authentisierung | Protokolleinstellungen

Netzwerkadapter

Adaptertyp	tun

Protokoll

Verschlüsselungsmethode	Blowfish mit CBC (128 bit)
Protokoll	UDP
lokaler VPN Port	1194
Partner VPN Port	1194

Verschiedenes

Die lokale IP-Adresse und der lokale Port werden fest eingestellt (bind)	☑
Erlaube dem Partner die IP-Adresse dynamisch zu ändern (float)	☐
Verwende die LZO Komprimierung (comp-lzo)	☑
Verbindung alle ...[sekunden] überprüfen (ping)	10
Verbindung nach ...[sekunden] Inaktivität neu starten (ping-restart)	60
Maximale Übertragungsgrösse (MTU) in ...[bytes] (tun-mtu)	1500
Alle UDP-Pakete die grösser sind als ...[bytes] werden in mehrere Pakete aufgeteilt (fragment)	
Erneuere den Sicherheitsschlüssel nach ...[sekunden] (reneg-sec)	3600
Sende mehr Ausgabeinformationen an das Protokolliersystem (verb 3)	☐

HTTP Proxy

Verwende als ausgehende Verbindung einen HTTP-Proxyserver	☐
Name des HTTP-Proxyserver (DNS oder IP)	
Port des HTTP-Proxyserver	8080
Anmeldename am HTTP-Proxyserver	
Anmeldepasswort am HTTP-Proxyserver	

Bezeichnung	**Funktion/Beschreibung**
Adaptertyp	Vorgabe, welches OpenVPN Device verwendet werden soll. Möglich sind folgende Punkte:
	tun: Bei Auswahl dieses Menüpunktes wird das tun-Device verwendet.
	tap: Bei Auswahl dieses Menüpunktes wird das tap-Device verwendet.
Verschlüsselungsmethode	Hier können Sie die Verschlüsselungsmethode auswählen. Diese Einstellung muss bei beiden VPN-Partnern gleich sein!
Protokoll	Es kann zwischen *„UDP“* und *„TCP“* gewählt werden. Die Standardeinstellung ist UDP. Wird ein HTTP-Proxy verwendet, gilt automatisch TCP.
Lokaler/Partner VPN-Port	Über die eingestellten Ports wird die OpenVPN Kommunikation geführt. In der Regel sind diese Ports gleich eingestellt. Standardmäßig ist es Port 1194.
Die lokale IP-Adresse und der lokale Port werden fest eingestellt (bind)	OpenVPN kann die Ports nicht dynamisch während der Verbindung ändern.
Erlaube dem Partner die IP-Adresse dynamisch zu ändern (float)	Mit dieser Option kann dem VPN-Partner erlaubt werden, seine IP-Adresse während der Verbindung zu ändern.
Verwende die LZO-Komprimierung (comp-lzo)	Komprimierungsmethode von OpenVPN
Verbindung alle … [sekunden] überprüfen (ping)	Falls der OpenVPN-Tunnel für n-Sekunden nicht in Benutzung war, wird ein Ping an den VPN-Partner gesendet.
Verbindung nach … [sekunden] Inaktivität neu starten (ping-restart)	Sollte der VPN-Partner nicht innerhalb von n-Sekunden auf den Ping antworten oder kein Datenpaket empfangen werden wird die VPN-Verbindung neu aufgebaut.
Maximale Übertragungsgröße (MTU) in … [bytes] (tun-mtu)	Gibt die maximale Paketgröße (Maximum Transmission Unit) an, die über die Verbindung gesendet werden kann. Größere Pakete werden in Teile zerlegt. Standardwert ist hier 1500.

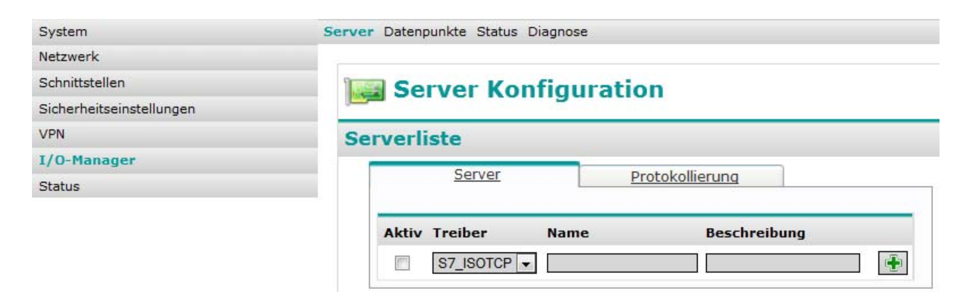
Alle UDP-Pakete die größer sind als … [bytes] werden in mehrere Pakete aufgeteilt (fragment)	Gibt an, dass übergroße Pakete in mehrere Teile zerlegt (fragmentiert) werden dürfen. Nur bei UDP-Protokoll erforderlich. Der Wert gibt die maximale Größe eines Paketes an.
Erneuere den Sicherheitsschlüssel nach … [sekunden] (reneg-sec)	Nach n-Sekunden wird ein neuer Schlüssel vereinbart. Standardmäßig ist dies auf 3600 gesetzt.
Sende mehr Ausgabeinformationen an das Protokollierungssystem (verb 3)	Dies entspricht der Einstellung „verb 3“ von OpenVPN. Standardmäßig ist diese Option ausgeschaltet. Durch aktivieren dieser Option erweitern Sie das Protokollierungssystem von OpenVPN, was dazu führt, dass genauere Informationen unter **Status – VPN-OpenVPN** angezeigt werden.
Verwende als ausgehende Verbindung einen HTTP-Proxyserver	Wenn die Internetverbindung des REX 300 über einen HTTP-Proxyserver erfolgen soll, dann muss diese Checkbox aktiviert sein.
Name des HTTP-Proxyserver (DNS oder IP)	Tragen Sie hier die IP-Adresse oder den DNS-Namen des zu verwendenden Proxy-Servers ein.
Port des HTTP-Proxyserver	Bitte geben Sie hier den Port ein, über den Ihr Proxyserver die Anfragen entgegennimmt (Bsp. 8080 oder 3128)
Anmeldename am HTTP-Proxyserver	Sollte eine Proxyauthentifizierung stattfinden, müssen Sie hier Ihren Benutzernamen für den Proxyserver eintragen.
Anmeldepasswort am HTTP-Proxyserver	Sollte eine Proxyauthentifizierung stattfinden, müssen Sie hier Ihr Passwort für den Proxyserver eintragen.

12 I/O Manager

12.1 Allgemeines

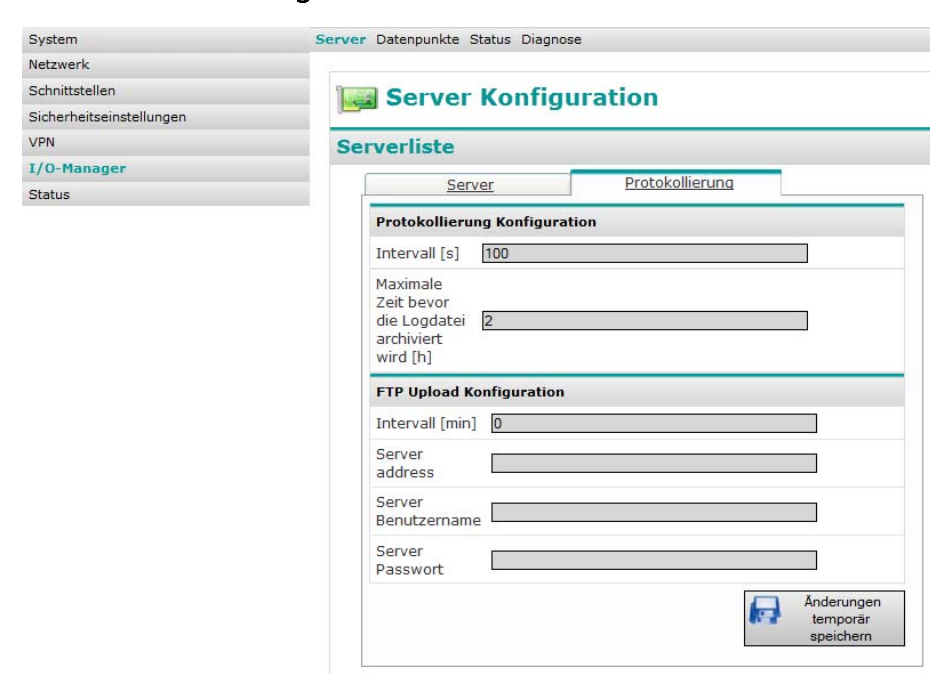
Der I/O-Manager ist ein im REX 300 integriertes System um Daten aus Steuerungssystemen auszulesen. Diese Daten können protokolliert und beobachtet werden.

12.1.1 Server



Bezeichnung	Funktion/Beschreibung
Server	Treiber S7-ISOTCP Die Felder Name und Beschreibung können frei gewählt werden. Im Feld "SPS IP-Adresse" muss die IP-Adresse der SPS eingetragen werden. Die SPS spezifischen Daten werden in den Feldern "SPS IP-Adresse" und "SPS Slot-Adresse" eingetragen. Die Slot-Adresse ist in den meisten Fällen die Zahl 2. Wird die Onboard-MPI/PROFIBUS Schnittstelle genutzt, so muss die LAN-IP-Adresse des Routers eingetragen werden. Zusätzlich muss auf jeden Fall RFC1006 aktiviert sein.

12.1.2 Protokollierung



Bezeichnung	Funktion/Beschreibung
Intervall [s]	Es werden in den angegebenen Intervall die Datenpunkte auf das Speichermedium geschrieben
Maximale Zeit bevor die Logdatei archiviert wird [h]	Nach dieser eingestellten Zeit in Stunden wird die Log-Datei auf jeden Fall archiviert und eine neue Log-Datei begonnen.
FTP Upload Konfiguration	Die protokollierten Datenpunkte können zusätzlich auf einem FTP-Server archiviert werden. Folgende Einstellungen sind dafür notwendig.
Intervall [min]	Es wird in den angegebenen Intervall die Log-Datei komprimiert und auf dem FTP-Server geladen. Die Log-Datei verbleibt zusätzlich auch auf dem Speichermedium (komprimiert).
Server Adresse	Geben Sie hier die Adresse des FTP-Servers an.
Server Benutzername	Geben Sie hier den Benutzernamen für Authentifizierung am FTP-Servers an.
Server Passwort	Geben Sie hier das Passwort für Authentifizierung am FTP-Servers an.

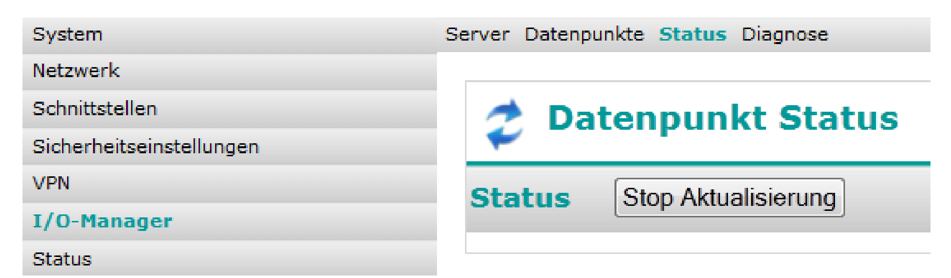
12.2 Datenpunkte



<table>
<tr><th>Bezeichnung</th><th>Funktion/Beschreibung</th></tr>
<tr><td colspan="2">Treiber S7-ISOTCP

Für diesen Treiber ist folgende Adressen-Syntax zu verwenden.
DBx.DBXy.z = Datenbaustein x, Datenbit y.z, BOOL
DBx.DBBy = Datenbaustein x, Datenbyte y, BYTE
DBx.DBWy = Datenbaustein x, Datenwort y, WORD
DBx.DBDy = Datenbaustein x, Datendoppelwort y, DWORD
My.z = Merkerbit y.z, BOOL
MBy = Merkerbyte y, BYTE
MWy = Merkerwort y, WORD
MDy = Merkerdoppelwort y, DWORD
Ey.z = Eingangsbit y.z, BOOL
EBy = Eingangsbyte y, BYTE
EWy = Eingangswort y, WORD
EDy = Eingangsdoppelwort y, DWORD
Ay.z = Ausgangsbit y.z, BOOL
ABy = Ausgangsbyte y, BYTE
AWy = Ausgangswort y, WORD
ADy = Ausgangsdoppelwort y, DWORD
PEy.z = Peripherieeingangsbit y.z, BOOL
PEBy = Peripherieeingangsbyte y, BYTE
PEWy = Peripherieeingangswort y, WORD
PEDy = Peripherieeingangsdoppelwort y, DWORD
Ty = Timer y, TIMER
Zy = Zaehler y, COUNTER</td></tr>
<tr><td>Anzeigeformat</td><td>Dieses Format wird bei der Statusanzeige und in den Protokollierungsdaten verwendet.</td></tr>
<tr><td>Beschreibung</td><td>Freies Beschriftungsfeld.</td></tr>
<tr><td>Intervall [x 100ms]</td><td>In diesem Intervall wird dieser Datenpunkt von der SPS gelesen.</td></tr>
<tr><td>Protokollierung</td><td>Ist diese Option aktiviert, ist dieser Datenpunkt für die Protokollierung freigegeben. Ist diese Option nicht aktiviert, wird der Datenpunkt nur auf der Statusanzeige dargestellt.</td></tr>
</table>

12.3 Status



In diesem Menü können die angelegten Datenpunkte abgefragt werden.

12.4 Diagnose



Hier werden im Fehlerfall entsprechende Meldungen ausgegeben

13 Statusmeldungen

13.1 Allgemeines

Beim Auftreten von Fehlern ist der Industrierouter anhand bestimmter Statusinfos zu analysieren. So wird z. B. durch Blinken der SF-LED angezeigt, dass am Router ein Systemfehler aufgetreten ist. Hierzu kann z. B. über **Status – System** anhand der Auflistung evtl. festgestellt werden, wo die Fehlerursache liegt.

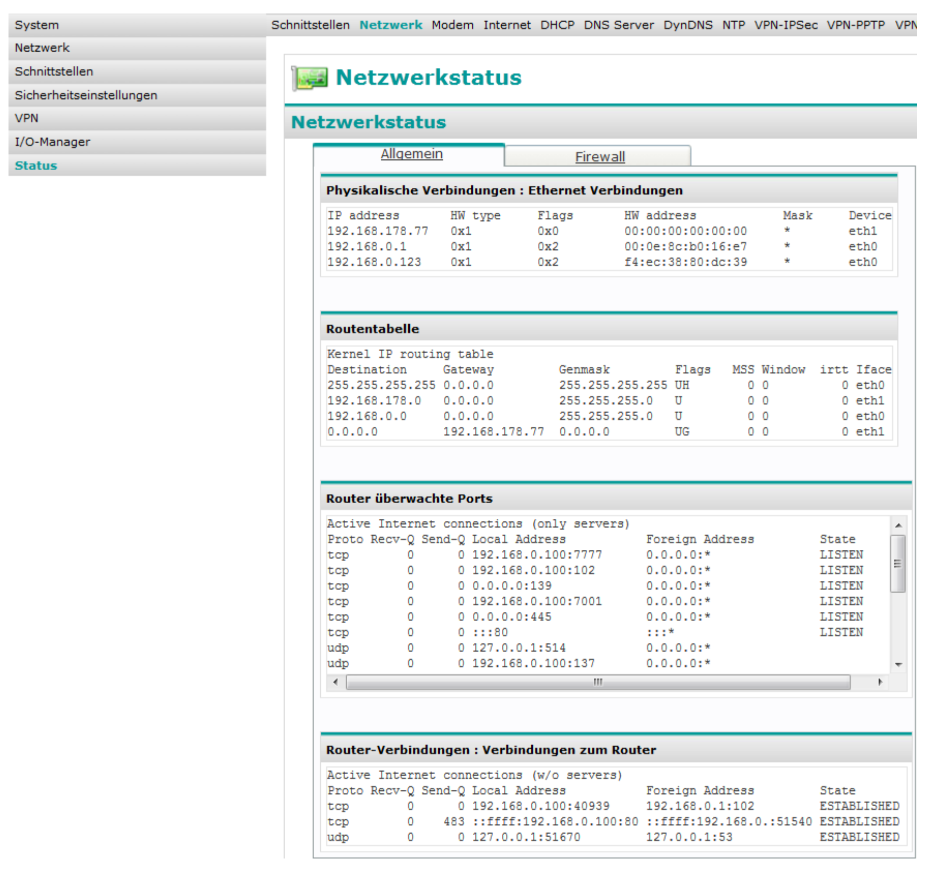
Nachfolgend die Beschreibung der verschiedenen Statusanzeigen:

13.2 Schnittstellen



Bezeichnung	Funktion/Beschreibung
WAN	Anzeige der Einstellungen am WAN-Anschluss (externer Anschluss) des Routers. Sobald der Router eine physikalische Verbindung zum Netzwerk hat oder ihm eine statische IP-Adresse zugewiesen wird, dann wird die IP-Adresse angezeigt. Die Anzahl empfangener und gesendeter Datenpakete wird angezeigt.
LAN	Anzeige der Einstellungen am LAN-Anschluss (lokaler Anschluss) des Routers. Die IP-Adresse wird dann angezeigt, wenn der Router eine physikalische Verbindung hat. Die Anzahl empfangener und gesendeter Datenpakete wird angezeigt.

13.3 Netzwerk



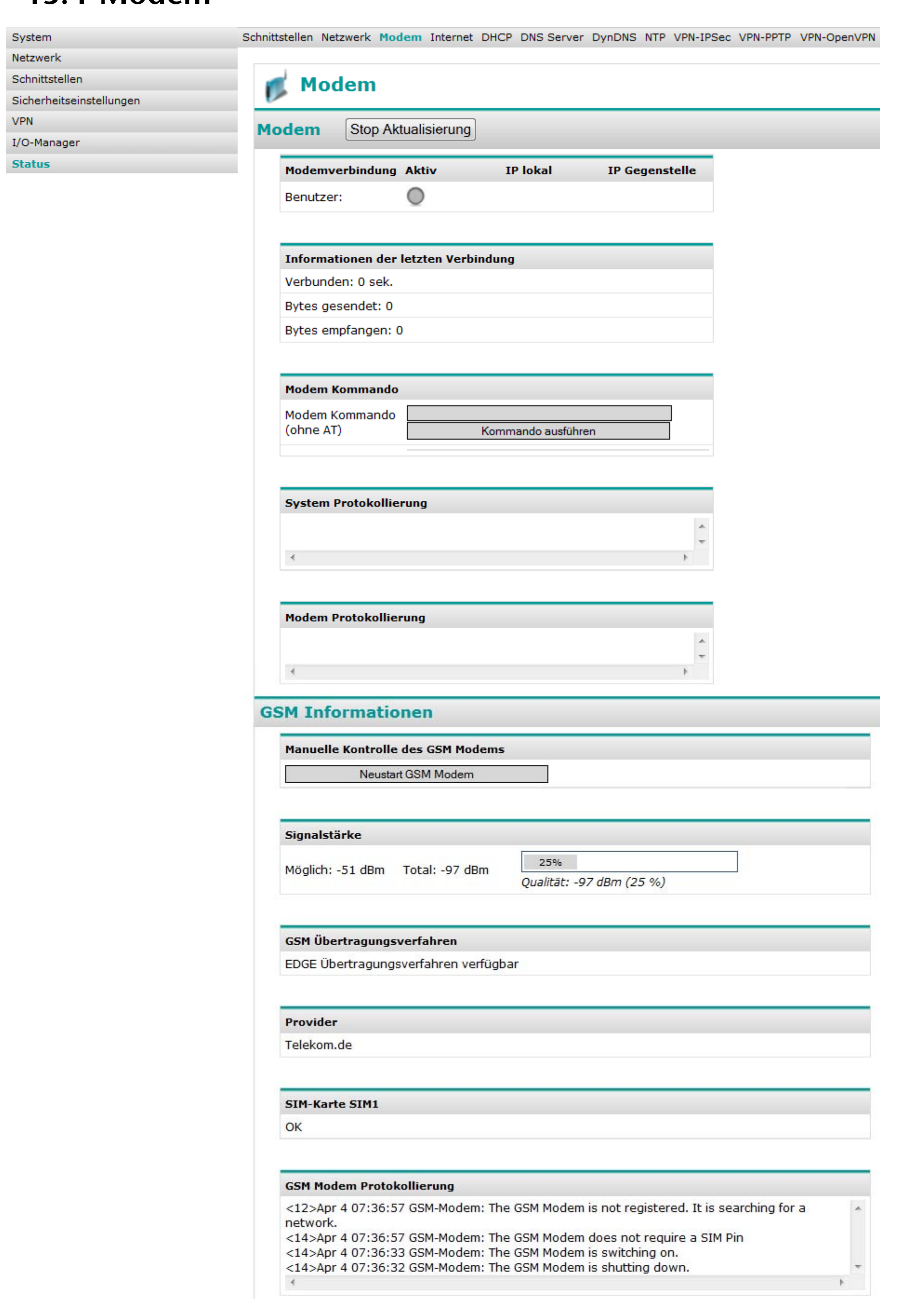
Allgemein:

Bezeichnung	Funktion/Beschreibung
Physikalische Verbindungen	Zeigt die physikalischen Verbindungen, über die der Router mit weiteren Rechnern verbunden ist.
Routentabelle	Zeigt alle Routen, die eingetragen sind und verwendet werden.
Router überwachte Ports	Zeigt sämtlich überwachte Ports an.
Router-Verbindungen	Zeigt sämtliche IP-Adressen mit Ports, z. B. von Rechnern an, die mit dem Router verbunden sind.

Firewall:

Anzeige aller Firewallregeln als Übersicht.

13.4 Modem

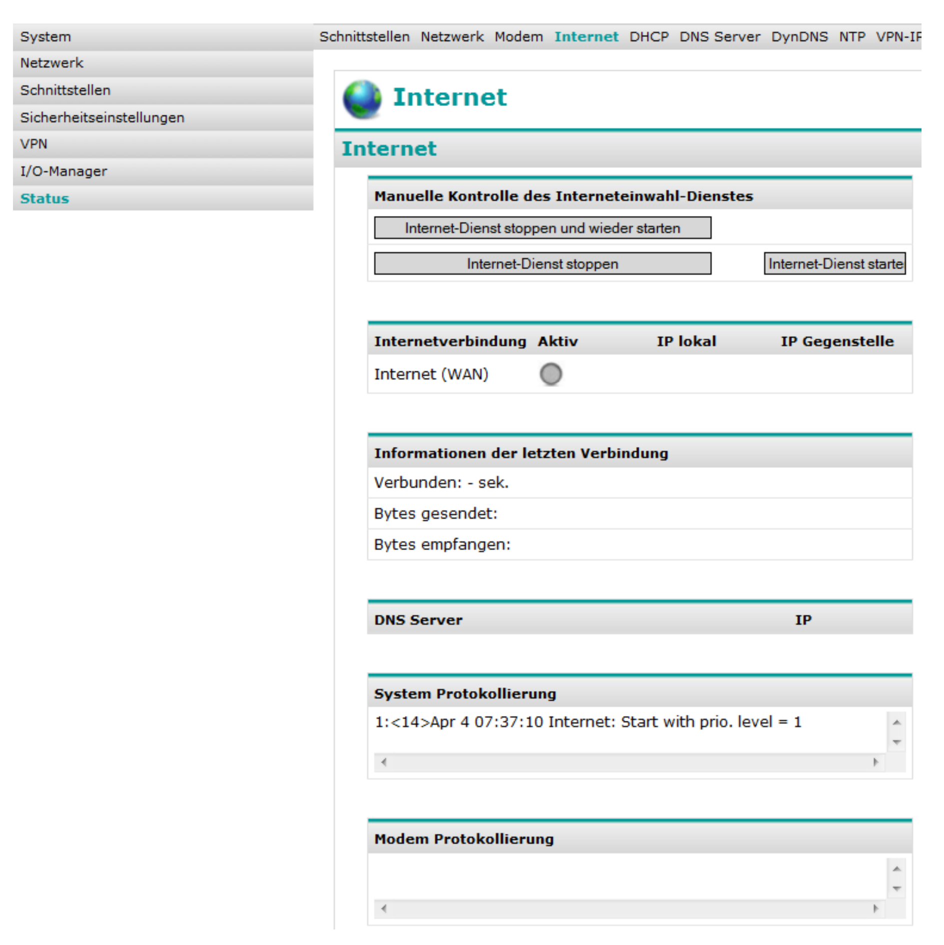


System
Netzwerk
Schnittstellen
Sicherheitseinstellungen
VPN
I/O-Manager
Status
Schnittstellen Netzwerk Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN
Modem
Modem
Stop Aktualisierung
Modemverbindung Aktiv IP lokal IP Gegenstelle
Benutzer:
Informationen der letzten Verbindung
Verbunden: 0 sek.
Bytes gesendet: 0
Bytes empfangen: 0
Modem Kommando
Modem Kommando (ohne AT)
Kommando ausführen
System Protokollierung
Modem Protokollierung
GSM Informationen
Manuelle Kontrolle des GSM Modems
Neustart GSM Modem
Signalstärke
Möglich: -51 dBm Total: -97 dBm
25%
Qualität: -97 dBm (25 %)
GSM Übertragungsverfahren
EDGE Übertragungsverfahren verfügbar
Provider
Telekom.de
SIM-Karte SIM1
OK
GSM Modem Protokollierung
<12>Apr 4 07:36:57 GSM-Modem: The GSM Modem is not registered. It is searching for a network.
<14>Apr 4 07:36:57 GSM-Modem: The GSM Modem does not require a SIM Pin
<14>Apr 4 07:36:33 GSM-Modem: The GSM Modem is switching on.
<14>Apr 4 07:36:32 GSM-Modem: The GSM Modem is shutting down.

Bezeichnung	Funktion/Beschreibung
Stop Aktualisierung	Mit diesem Button kann die automatische Aktualisierung der Seite gestoppt werden.
Modemverbindung	Es wird angezeigt, welcher Benutzer sich per Modem auf den Router eingewählt hat. Bei erfolgreicher Wählverbindung werden IP-Adresse des PPP-Servers und des PPP-Clients (Gegenstelle) angezeigt. Hierbei handelt es sich immer um eingehende Verbindungen. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis symbolisiert.
Informationen der letzten Verbindung	Zeigt die Verbindungszeit und die Anzahl der gesendeten und empfangenen Bytes der letzten Verbindung an, solange der Router nicht neu gestartet oder zwischenzeitlich ausgeschaltet wurde.
Modem Kommando	Hiermit kann dem internen Modem direkt ein Befehl erteilt werden. Benutzen Sie diese Funktion nur nach Anweisung des Supportpersonals von Systeme Helmholz!
System Protokollierung	Zeigt die Art der Verbindung und die vergebenen IP- und DNS-Adressen an.
Modem Protokollierung	Es wird angezeigt, welche Befehle zur Initialisierung an das Modem geschickt werden und welchen Status der Verbindungsaufbau hat. Des Weiteren werden hier auch die Fehlermeldungen beim Verbindungsaufbau angezeigt.
Manuelle Kontrolle des GSM Modems	Mit diesem Button können Sie das interne Modem neu starten. Benutzen Sie diese Funktion nur nach Anweisung des Supportpersonals von Systeme Helmholz!
Signalstärke	Hiermit wird die momentane Netzverfügbarkeit in Prozent und dBm angegeben. Wenn Sie einen REX 300 mit GSM-Modem besitzen, wird das Gerät automatisch das entsprechend verfügbare Netz auswählen. (z. B. GPRS oder EDGE)

GSM Übertragungsverfahren	Hier wird Ihnen das aktuell mögliche Übertragungsverfahren angezeigt. Möglich sind:
	GSM
	GPRS
	EDGE
	UMTS
	HSDPA
Provider	Hier sehen Sie den momentanen Mobilfunkanbieter (z. B. T Mobile D wie in der Abbildung zu sehen)
SIM-Karte	Hier wird der Status Ihrer SIM-Karte im REX 300 angezeigt.
GSM Modem Protokollierung	Hier werden alle Ereignisse und Fehler des GSM-Modems eingetragen.

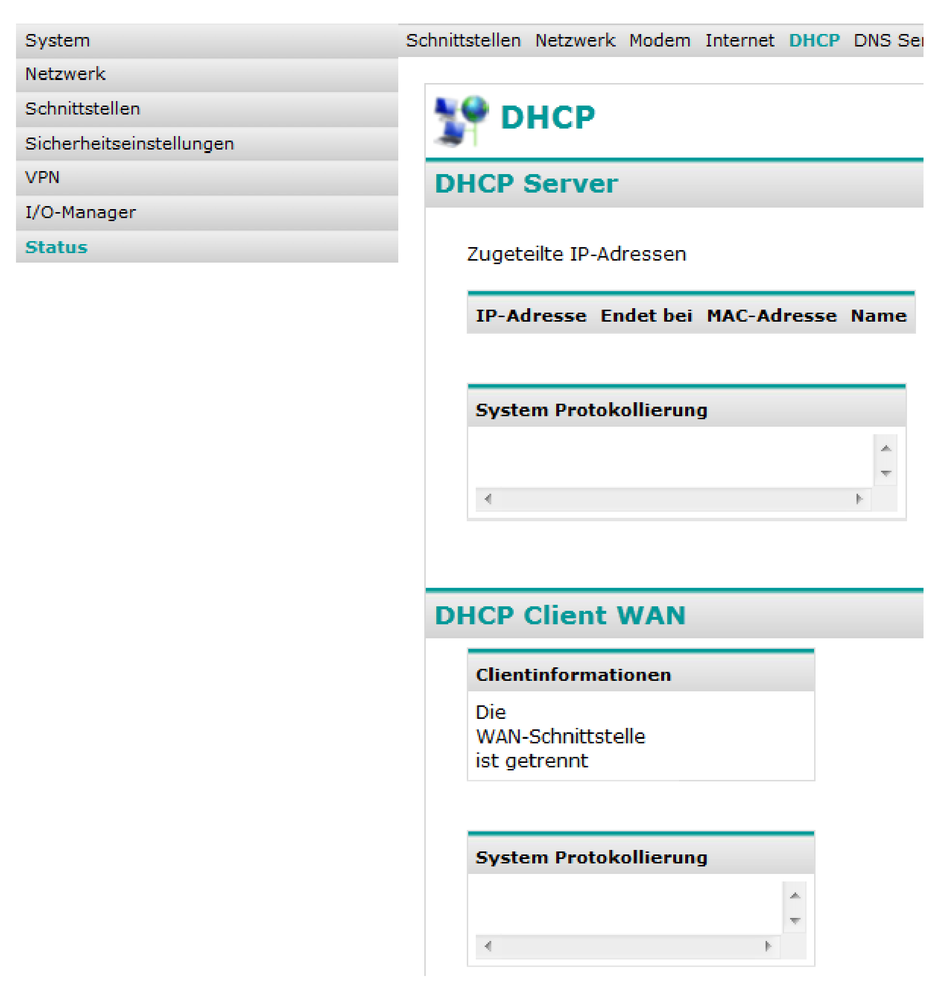
13.5 Internet



Bezeichnung	Funktion/Beschreibung
Internet	Hier werden ausgehende Verbindungen ins Internet angezeigt. Dies können sowohl ausgehende Verbindungen über das Modem als auch Verbindungen über WAN sein. Es werden lokale und die IP-Adressen der Gegenstelle angezeigt. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis symbolisiert. Hier kann zusätzlich die Internetverbindung manuell getrennt oder initiiert werden. Es wird jedoch nicht empfohlen, diese Buttons zu verwenden, außer Sie werden von einem Supportmitarbeiter dazu aufgefordert.
Informationen der letzten Verbindung	Zeigt die Verbindungszeit und die Anzahl der gesendeten und empfangenen Bytes der letzten Verbindung an, solange der Router nicht neu gestartet oder zwischenzeitlich ausgeschaltet wurde.

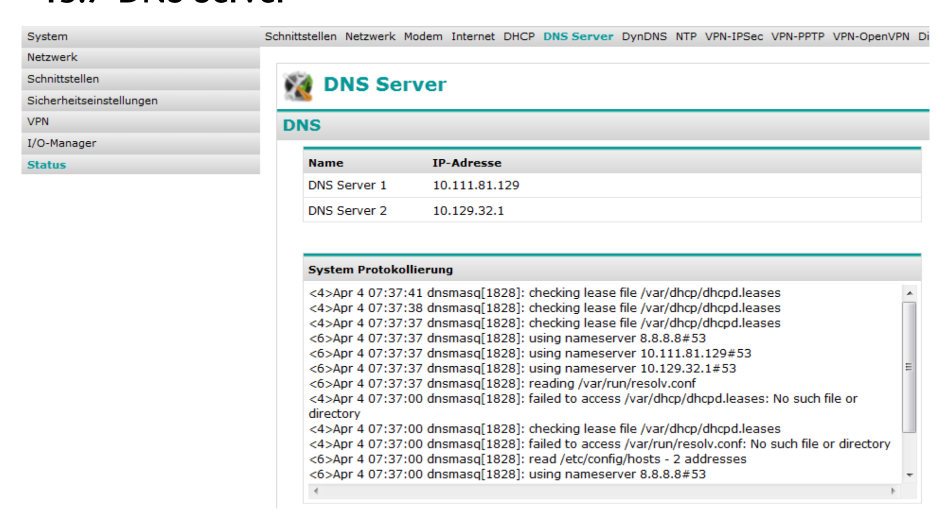
DNS Server	Zeigt die IP-Adresse des verwendeten DNS-Servers an. Dieser wird i. d. R. bei einer Internetverbindung über Modem vom Provider zugewiesen.
Systemprotokollierung	Zeigt die Art der Verbindung und die vergebenen IP- und DNS-Adressen an.
Modemprotokollierung	Es wird angezeigt, welche Befehle zur Initialisierung an das Modem geschickt werden und welchen Status der Verbindungsaufbau hat. Des Weiteren werden hier auch die Fehlermeldungen beim Verbindungsaufbau angezeigt.

13.6 DHCP



Bezeichnung	Funktion/Beschreibung
DHCP Server	Hier werden die IP-Adressen, die der DHCP-Server an angeschlossene Clients vergibt, aufgelistet.
Systemprotokollierung	Zeigt die IP-Adressen, die der DHCP vergibt und welche IP-Adressen unzulässig sind.
Clientinformationen	Informationen über angeschlossene Clients am WAN-Anschluss.
Systemprotokollierung	Hier werden alle Ereignisse und Fehler, die den DHCP-Server und -Client betreffen, aufgelistet.

13.7 DNS Server



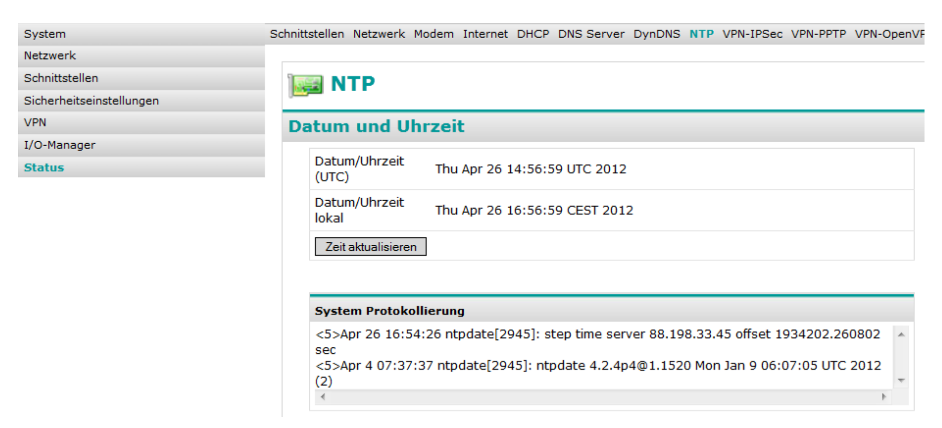
Bezeichnung	Funktion/Beschreibung
Name	Anzeige des Namens vom DNS-Server, falls nicht vom Internetserviceprovider vergeben.
IP-Adresse	Anzeige der IP-Adresse des DNS-Servers, falls nicht vom Internetserviceprovider vergeben.
Systemprotokollierung	Anzeige der Arbeitsschritte, die der DNS-Server ausführt.

13.8 DynDNS



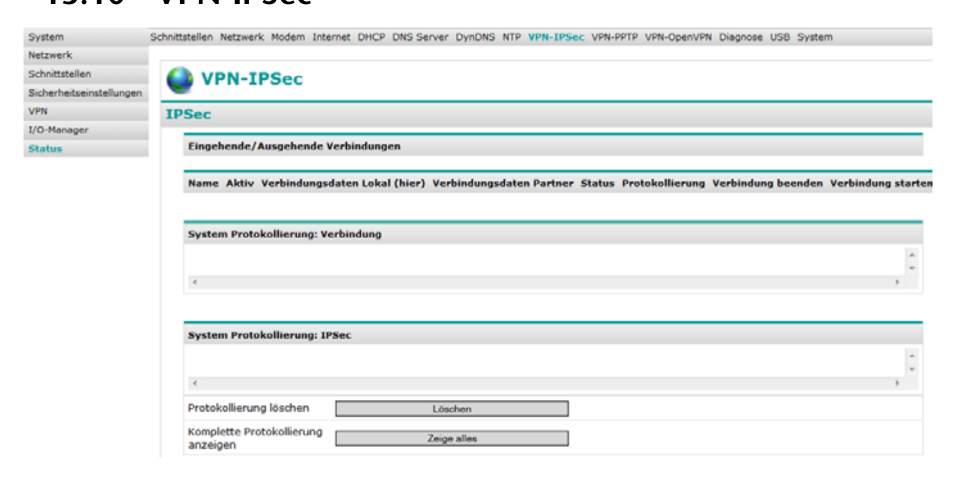
Bezeichnung	Funktion/Beschreibung
Aktualisierte IP-Adresse	Anzeige der momentan aktuellen IP-Adresse, die dem Router vom Internet Service Provider zugewiesen wurde.
Systemprotokollierung	Hier werden alle Ereignisse und Fehler, die den DynDNS-Dienst betreffen, angezeigt.

13.9 NTP



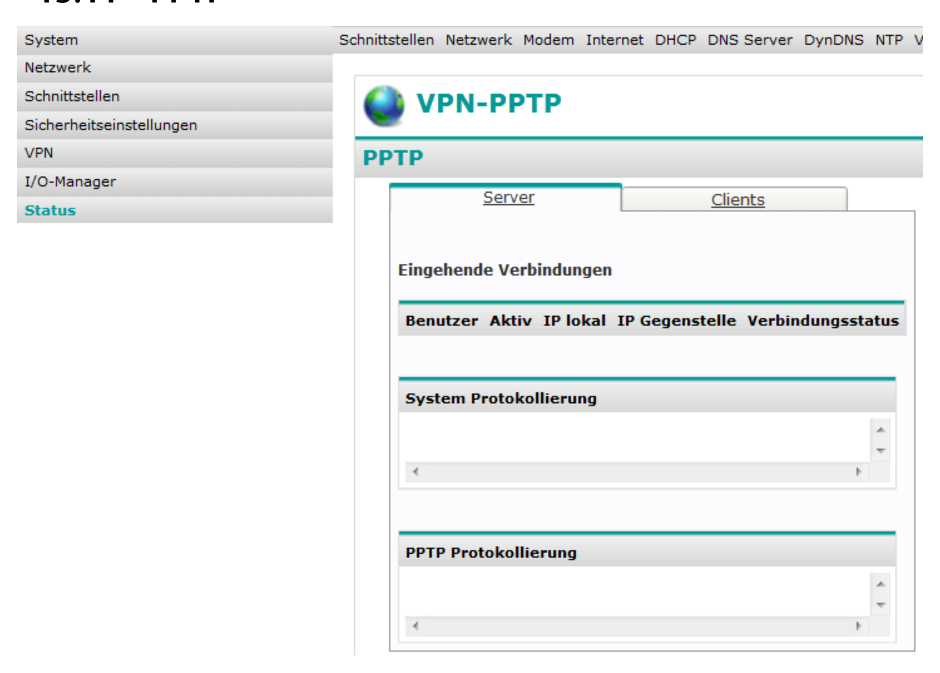
Bezeichnung	Funktion/Beschreibung
Datum/Uhrzeit (UTC)	Anzeige der aktuellen Systemzeit in Universal Time Coordinates (UTC).
Datum/Uhrzeit lokal	Anzeige der Uhrzeit anhand der Einstellungen der Zeitzone.
Systemprotokollierung	Hier werden alle Benachrichtigungen und Fehlermeldungen des NTP-Dienstes angezeigt.

13.10 VPN-IPSec



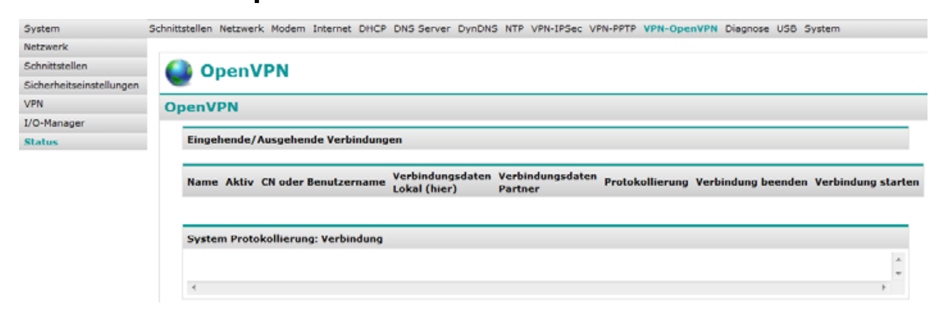
Bezeichnung	Funktion/Beschreibung
Eingehende/Ausgehende Verbindungen	Hier werden sowohl die eingehenden als auch die ausgehenden IPSec-VPN Verbindungen des Routers angezeigt. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis symbolisiert. Zusätzlich wird die Verbindungsdauer und der eingewählte Benutzer angezeigt. Nach Trennung der Verbindung wird angezeigt, wie lange die Verbindung aktiv war. Des Weiteren können hier Verbindungen manuell getrennt oder aufgebaut werden. Es wird empfohlen, diese Buttons nur auf Anweisung von einem Supportmitarbeiter zu verwenden.
Systemprotokollierung	Hier werden alle Benachrichtigungen und Fehlermeldungen der Verbindung sowie des IPSec-Dienstes angezeigt.
Protokollierung löschen	Mit diesem Button kann die angezeigte Protokollierung gelöscht werden.
Komplette Protokollierung anzeigen	Mit diesem Button wird Ihnen eine ausführlichere Version der Protokollierung angezeigt.

13.11 PPTP



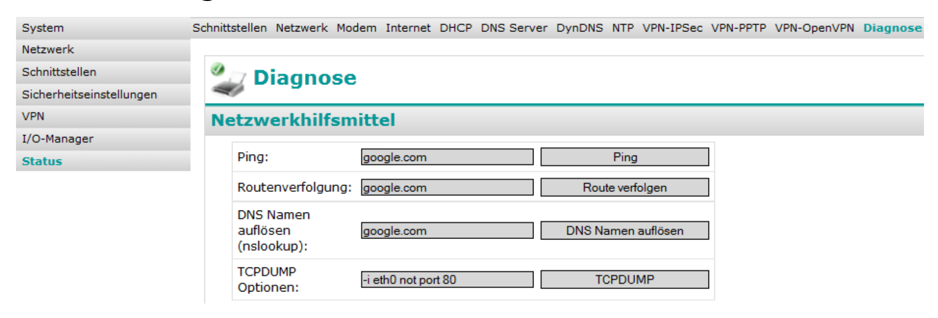
Bezeichnung	Funktion/Beschreibung
Server	Hier werden die eingehenden PPTP-VPN-Verbindungen des Routers aufgeführt. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis symbolisiert. Es werden Verbindungsdauer, der eingewählte Benutzer, lokale und entfernte IP-Adresse angezeigt. Nach Trennung der Verbindung wird angezeigt, wie lange die Verbindung aktiv war.
Client	Hier werden die vom Router ausgehenden PPTP-VPN-Verbindungen angezeigt. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis dargestellt. Es werden Verbindungsdauer, der eingewählte Benutzer, lokale und entfernte IP-Adresse angezeigt. Die Verbindungen werden protokolliert. Nach Trennung der Verbindung wird angezeigt, wie lange die Verbindung aktiv war.
System Protokollierung	Hier werden alle Benachrichtigungen und Fehlermeldungen des PPTP-Dienstes angegeben.

13.12 VPN-OpenVPN



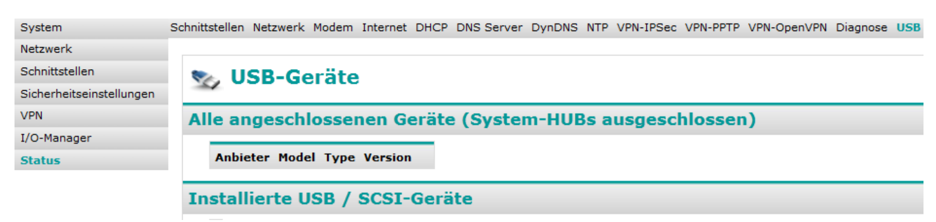
Bezeichnung	**Funktion/Beschreibung**
Eingehende/Ausgehende Verbindungen	Hier werden sowohl die eingehenden als auch die ausgehenden OpenVPN-VPN Verbindungen des Routers angezeigt. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis symbolisiert. Hier werden außerdem Name, lokale- und Partner-IP-Adresse angezeigt. Des Weiteren können hier Verbindungen manuell getrennt oder aufgebaut werden. Es wird empfohlen, diese Buttons nur auf Anweisung von einem Supportmitarbeiter zu verwenden.
Systemprotokollierung	Hier werden alle Benachrichtigungen und Fehlermeldungen der Verbindung sowie des OpenVPN-Dienstes angezeigt.

13.13 Diagnose



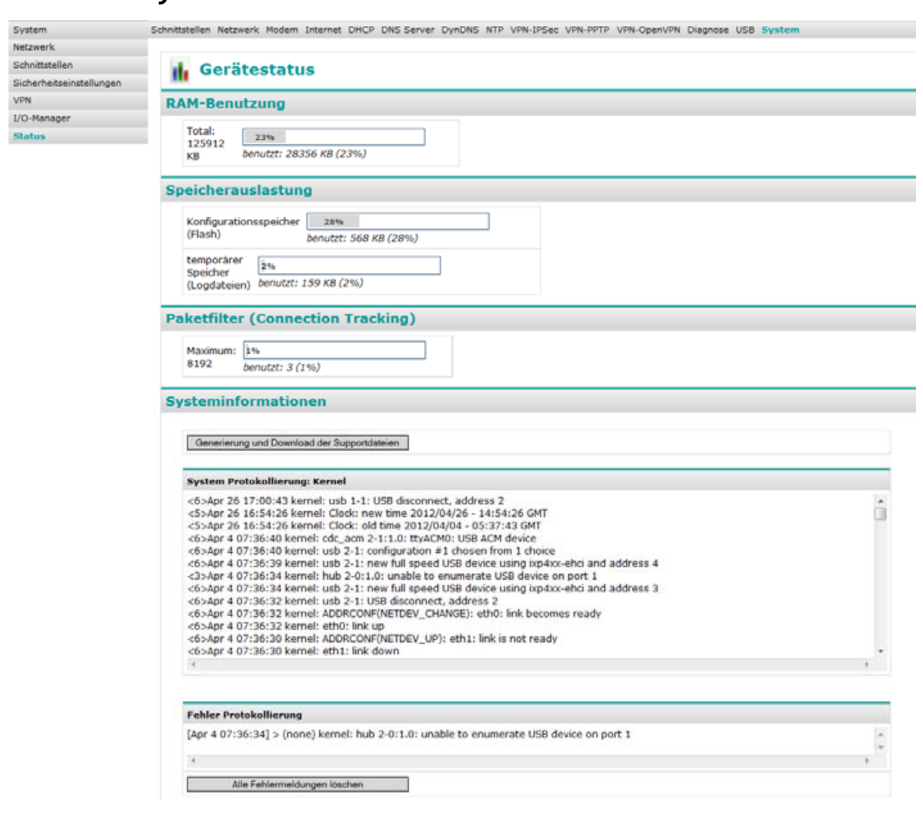
Bezeichnung	Funktion/Beschreibung
Ping	Nach Eingabe einer Internet- oder IP-Adresse kann über den Ping-Befehl festgestellt werden, ob die entsprechende Adresse erreichbar ist. So kann z. B. leicht festgestellt werden, ob eine Internetverbindung vorhanden ist und falls ein DNS-Name wie z. B. www.helmholz.de eingegeben wurde, die Namensauflösung funktioniert.
Routenverfolgung	Mit diesem Befehl erhält man noch mehr Informationen über die Netzwerkverbindung zwischen Router und einem entfernten Rechner oder einem weiteren Router. Hier wird eine Routenverfolgung vorgenommen und sichtbar gemacht.
DNS-Namen auflösen	Mit dieser Funktion kann geprüft werden, ob eine Namensauflösung stattfindet. Sollte diese Funktion in einer Fehlermeldung enden, dann prüfen Sie, ob in Ihrem REX 300 eine DNS-Serveradresse unter **Netzwerk – DNS** eingetragen ist oder ob der DNS-Server Ihres Netzwerkes erreichbar ist.
TCPDUMP	Dies ist eine Funktion zum Überwachen und Auswerten von Netzwerkverkehr. Eine ausführliche Anleitung zur Funktion TCPDUMP finden Sie auf www.tcpdump.org

13.14 USB



Bezeichnung	Funktion/Beschreibung
Alle angeschlossenen Geräte (System-HUBs ausgeschlossen)	Bei angeschlossenem USB-Speicher, werden Anbieter, Modell, Typ und Version angezeigt.
Installierte USB/SCSI-Geräte	Darunter folgt eine Anzeige wie der USB-Speicher in das Dateisystem des Routers eingebunden ist und welches Dateisystem auf dem USB-Speicher angelegt ist.

13.15 System



Bezeichnung	Funktion/Beschreibung
RAM-Benutzung	Anzeige des momentan verwendeten RAM-Speichers im Router.
Speicherauslastung	Zeigt die Auslastung des Konfigurationsspeichers und des temporären Speichers an.
Paketfilter	Zeigt die Auslastung des Paketfilters an.

Systeminformationen	Über die Systeminformationen können evtl. Fehlerursachen am Router herausgefunden werden. Blinkt z. B. die SF-LED an der Frontseite, dann kann hier evtl. anhand der Protokollierung herausgefunden werden, wo die Fehlerursache liegt.
Generierung und Download der Supportdateien	Dieser Button dient der Zusammenstellung von Diagnoseinformationen für unseren Support. Wenn Sie diesen Button betätigen, wird eine Datei mit allen nötigen Informationen zusammengepackt und zum speichern auf Ihrem PC freigegeben. Diese Datei können Sie dann an unseren Support senden.
Fehlerprotokollierung	Hier werden alle Fehler solange gespeichert, bis der Button „Alle Fehlermeldungen löschen“ betätigt wird. Zusätzlich wird auf der Seite **System – Info** und der Assistenzseite der zuletzt aufgetretene Fehler angezeigt. Um von einer der beiden Seiten direkt zum Fehlerspeicher zu gelangen, muss nur auf die letzte Fehlermeldung geklickt werden.

14 Werksseitige Einstellungen bei Auslieferung

14.1 Benutzername und Passwort



Es wird empfohlen, Benutzername und Passwort zu ändern!

Der Router wird mit folgendem angelegten Benutzernamen und Passwort ausgeliefert:

Benutzername: helmholz

Passwort: router

14.2 IP-Adresse des Routers

Der Router ist werksseitig auf folgende IP-Adresse eingestellt:

IP-Adresse: 192.168.0.100

Subnetzmaske: 255.255.255.0

15 Werkseinstellungen laden



Sichern Sie vor dem Zurücksetzen Ihre Konfiguration. Durch das Zurücksetzen sind alle vorher vorgenommenen Einstellungen nicht mehr vorhanden.

Befolgen Sie die unten aufgeführten Schritte, um den Industrierouter wieder auf die Werkseinstellungen zurückzusetzen:

1. Gerät einschalten
2. Warten bis Rdy-LED blinkt
3. Dial Out Taste drücken und gedrückt halten, bis die TxD-LED leuchtet
4. Dial Out Taste erneut drücken (RxD-LED leuchtet)
5. Dial Out Taste nochmals drücken (TxD-LED leuchtet orange)
6. Zum Schluss ein letztes Mal die Dial Out Taste drücken



Die IP-Adresse des REX 300 wird auf 192.168.0.100 zurückgesetzt. Dementsprechend sind die Netzwerkeinstellungen des angeschlossenen Rechners zu ändern.

Nun ist die individuell eingestellte Konfiguration gelöscht. Der Industrierouter ist wieder in Werkseinstellung und kann neu konfiguriert werden.

16 Modeminitialisierung

16.1 Allgemeines

Die Befehle können in der Eingabeoberfläche (Modemeinstellungen) in die beiden Felder *„Modem Initialisierung"* eingetragen werden.

Das Präfix besteht immer aus den Zeichen „AT".
Dieses muss nicht in das Feld eingegeben werden.

Der Befehl setzt sich aus einzelnen Zeichen zusammen, die wie folgt beschrieben werden. Der Befehl besteht aus einem Kürzel und gegebenenfalls zugehörigen Werten.

Es wird Groß- und Kleinschreibung akzeptiert. Mehrere Befehle können zu einer Befehlszeile zusammengefasst werden.

Beispiel: L1M1\N5

16.2 Befehle des Analog-Modems

B — Kommunikationsstandard auswählen

B0	CCITT Modulation
B1	Bell Modulation

\B — Behandlung des Breaksignals

\Bn Break Signal zur Gegenstelle senden
n=0-9 in 100 ms Einheiten (Standard \B3)
Nur bei nicht fehlerkorrigierter Verbindung möglich.

%C — Einstellung der Datenkompression

%C0	Datenkompression inaktiv
%C1	Datenkompression aktiv

+GCI — Länderspezifische Einstellung

Mit diesem Befehl wird das analoge Modem auf die länderspezifische Einstellung konfiguriert.
Bsp. +GCI=B5 (Codes siehe Länderliste Kapitel 15.1)

L — Lautsprecher Lautstärke

L0,1	geringe Lautstärke
L2	mittlere Lautstärke
L3	hohe Lautstärke

M	Lautsprecher Mode	
	M0	Lautsprecher immer aus.
	M1	Lautsprecher ein, bis Datenträgersignal erkannt ist.
	M2	Lautsprecher ein, wenn das Modem wählbereit ist.
	M3	Lautsprecher aus, währen die Rufnummer gewählt wird, dann nachdem Wählen ein, bis Datenträgersignal erkannt wird.

+MS Modulationsart auswählen

Mit diesem Kommando wird die Modulationsart und die Baudraten, die zwischen dem lokalen und dem entfernten Modem ausgehandelt werden, eingestellt.

Syntax:
+ms=[<carrier>[,<automode>[,<min_tx_rate>[,
<max_tx_rate>[,<min_rx_rate>[,<max_rx_rate>]]]]]

Beispiel: AT+MS= V34,1,9600.33600.9600.33600

Modulation	<carrier>	Mögliche Baudraten
Bell 103	B103	300
Bell 212	B212	1200 Rx 75 Tx oder 75 Rx/1200 Tx
V.21	V21	300
V.22	V22	1200
V.22 bis	V22B	1200, 2400
V.23	V23C	1200
V.32	V32	4800, 9600
V.32 bis	V32B	4800, 7200, 9600, 12000, 14400
V.34	V34	2400, 4800,7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, 31200, 33600

Automode 0 = deaktiviert
1 = aktiviert (Standard)

+MS? Anzeige der aktuellen Einstellung

\N Auswahl der Fehlerkorrektur

\N0 Fehlerkorrektur ausgeschaltet.

\N1 Transparente Übertragung beliebiger Datenbreiten über die serielle Schnittstelle ohne Datenpufferung und Fehlerkorrektur.

\N2 V.42LAP-M oder MNP 4 Fehlerkorrektur. Kann keine fehlergesicherte Verbindung aufgebaut werden, legt das Modem auf.

\N3 V.42LAP-M oder MNP 4 Fehlerkorrektur. Kann keine fehlergesicherte Verbindung aufgebaut werden, wird eine nicht fehlergesicherte Verbindung angestrebt.

\N4 V.42LAP-M Fehlerkorrektur, ist dies nicht möglich legt das Modem auf.

\N5 MNP Fehlerkorrektur, ist dies nicht möglich legt das Modem auf.

X Ausgabe der Meldungen, Wähltonerkennung

Dieses Kommando steuert, wie das Modem auf Wählton und Besetztsignal reagiert und wie es die CONNECT Meldung anzeigt.

X0 Keine Besetzt und Wähltonerkennung d. h. bei einem erfolglosen Wählversuch wird NO CARRIER angezeigt. Meldungen: OK, CONNECT, RING, NO CARRIER, ERROR und NO ANSWER werden angezeigt.

X1 wie X0 aber CONNECTxxx Meldungen mit Geschwindigkeitsangabe.

X2 Besetzttonerkennung deaktiviert, Wähltonerkennung aktiviert. Meldungen: OK, CONNECT, RING, NO CARRIER, ERROR, NO ANSWER und NO DIAL TONE werden angezeigt.

X3 Besetzttonerkennung aktiviert, Wähltonerkennung deaktiviert.
Meldungen: OK, CONNECT xxx, RING, NO CARRIER, ERROR und NO ANSWER werden angezeigt.

X4 Besetzt- und Wähltonerkennung aktiviert.
Meldungen: OK, CONNECT xxx, RING, NO CARRIER, ERROR, NO ANSWER und NO DIAL TONE werden angezeigt.

16.3 Befehle des ISDN Terminal Adapters (TA)

B	Festlegung des Übertragungsprotokolles im B-Kanal	
	B0	V110 asynchron
	B3	PPP asynchron zu synchron Konvertierung (PPP asynchron single link)
	B4	HDLC transparent
	B5	Byte transparent (B-Kanal Daten)
	B10	X.75 transparent
	B13	V.120
	B20	X.31 B-Kanal (X.25 B-Kanal)
	B21	X.31 D-Kanal
N	Legt Übertragungsrate im V.110 Modus fest	
	N0	Verbindungsgeschwindigkeit automatisch
	N1	Verbindungsgeschwindigkeit 1.200 bit/s
	N2	Verbindungsgeschwindigkeit 2.400 bit/s
	N3	Verbindungsgeschwindigkeit 4.800 bit/s
	N4	Verbindungsgeschwindigkeit 9.600 bit/s
	N5	Verbindungsgeschwindigkeit 19.200 bit/s
#Z	Definiert die MSN (Multiple Subscriber Number)	
	Ist die Nummer auf „*“ (Stern) gesetzt (Standardeinstellung), wird jeder Anruf angenommen. In der Regel muss aber eine MSN eingegeben werden, da dies die meisten TK-Anlagen verlangen. Außerdem muss die MSN für den Datendienst freigegeben werden.	
	#Z=n Setzt MSN auf n	
	Bsp:	AT#Z=870

17 Anhang

17.1 Ländercodes für analoge Modems

Nr.	Land	Einstellung
1	Afghanistan	B5
2	Albania(AL)	B5
3	Algeria(DZ)	B5
4	American Samoa(AS)	B5
5	Andorra(AD)	B5
6	Angola(AO)	B5
7	Anguilla(AI)	B5
8	Antarctica(AQ)	B5
9	Antigua and Barbuda(AG)	B5
10	Argentina(AR)	07
11	Armenia(AM)	B5
12	Aruba(AW)	B5
13	Australia(AU)	09
14	Austria(AT)	FD
15	Azerbaijan(AZ)	B5
16	Bahamas(BS)	B5
17	Bahrain(BH)	B5
18	Bangladesh(BD)	B5
19	Barbados(BB)	B5
20	Belarus(BY)	B5
21	Belgium(BE)	FD
22	Belize(BZ)	B5
23	Benin(BJ)	B5
24	Bermuda(BM)	B5
25	Bhutan(BT)	B5
26	Bolivia(BO)	B5
27	Bosnia and Herzegowina(BA)	B5
28	Botswana(BW)	B5
29	Bouvet Island(BV)	B5
30	Brazil(BR)	16
31	British Indian Ocean Territory(IO)	B5
32	Brunei Darussalam(BN)	B5
33	Bulgaria(BG)	FD
34	Burkina Faso(BF)	B5
35	Burundi(BI)	B5
36	Cambodia(KH)	B5
37	Cameroon(CM)	B5
38	Canada(CA)	B5
39	Cape Verde(CV)	B5
40	Cayman Islands(KY)	B5
41	Central African Republic(CF)	B5
42	Chad(TD)	B5
43	Chile(CL)	B5
44	China(CN)	B5
45	Christmas Island(CX)	B5

Nr.	Land	Einstellung
46	Cocos (Keeling) Islands(CC)	B5
47	Colombia(CO)	B5
48	Comoros(KM)	B5
49	Congo(CG)	B5
50	Cook Islands(CK)	B5
51	Costa Rica(CR)	B5
52	Cote D'Ivoire(CI)	B5
53	Croatia(HR)	B5
54	Cuba(CU)	B5
55	Cyprus(CY)	FD
56	Czech Republic(CZ)	FD
57	Denmark(DK)	FD
58	Djibouti(DJ)	B5
59	Dominica(DM)	B5
60	Dominican Republic(DO)	B5
61	East Timor(TP)	B5
62	Ecuador(EC)	B5
63	Egypt(EG)	B5
64	El Salvador(SV)	B5
65	Equatorial Guinea(GQ)	B5
66	Eritrea(ER)	B5
67	Estonia(EE)	FD
68	Ethiopia(ET)	B5
69	Falkland Islands (Malvinas)(FK)	B5
70	Faroe Islands(FO)	B5
71	Fiji(FJ)	B5
72	Finland(FI)	FD
73	France(FR)	FD
74	France-Metropolitan(FX)	FD
75	French Guiana(GF)	B5
76	French Polynesia	B5
77	French Southern Territories(TF)	B5
78	Gabon(GA)	B5
79	Gambia(GM)	B5
80	Georgia(GE)	B5
81	Germany(DE)	FD
82	Ghana(GH)	B5
83	Gibraltar(GI)	B5
84	Greece(GR)	FD
85	Greenland(GL)	B5
86	Grenada(GD)	B5
87	Guadeloupe(GP)	B5
88	Guam(GU)	B5
89	Guatemala(GT)	B5
90	Guinea(GN)	B5
91	Guinea-Bissau(GW)	B5
92	Guyana(GY)	B5
93	Haiti(HT)	B5
94	Heard and Mc Donald Islands(HM)	B5
95	Honduras(HN)	B5

Nr.	Land	Einstellung
96	Hong Kong(HK)	99
97	Hungary(HU)	FD
98	Iceland(IS)	FD
99	India(IN)	B5
100	Indonesia(ID)	99
101	Iran(Islamic Republic of)(IR)	B5
102	Iraq(IQ)	B5
103	Ireland(IE)	FD
104	Israel(IL)	B5
105	Italy(IT)	FD
106	Jamaica(JM)	B5
107	Japan(JP)	00
108	Jordan(JO)	B5
109	Kazakhstan(KZ)	B5
110	Kenya(KE)	B5
111	Kiribati(KI)	B5
112	Korea-Democratic People's Republic(KP)	B5
113	Korea-Republic of(KR)	B5
114	Kuwait(KW)	B5
115	Kyrgyzstan(KG)	B5
116	Lao People's Democratic Republic(LA)	B5
117	Latvia(LV)	FD
118	Lebanon(LB)	B5
119	Lesotho(LS)	B5
120	Liberia(LR)	B5
121	Libyan Arab Jamahiriya(LY)	B5
122	Liechtenstein(LI)	FD
123	Lithuania(LT)	FD
124	Luxembourg(LU)	FD
125	Macau(MO)	B5
126	Macedonia(MK)	B5
127	Madagascar(MG)	B5
128	Malawi(MW)	B5
129	Malaysia(MY)	6C
130	Maldives(MV)	B5
131	Mali(ML)	B5
132	Malta(MT)	FD
133	Marshall Islands(MH)	B5
134	Martinique(MQ)	B5
135	Mauritania(MR)	B5
136	Mauritius(MU)	B5
137	Mayotte(YT)	B5
138	Mexico(MX)	B5
139	Micronesia(Federated States of)(FM)	B5
140	Moldova-Republic of(MD)	B5
141	Monaco(MC)	B5
142	Mongolia(MN)	B5
143	Montserrat(MS)	B5
144	Morocco(MA)	B5
145	Mozambique(MZ)	B5

Nr.	Land	Einstellung
146	Myanmar(MM)	B5
147	Namibia(NA)	B5
148	Nauru(NR)	B5
149	Nepal(NP)	B5
150	Netherlands(NL)	FD
151	Netherlands Antilles(AN)	FD
152	New Caledonia(NC)	B5
153	New Zealand(NZ)	7E
154	Nicaragua(NI)	B5
155	Niger(NE)	B5
156	Nigeria(NG)	B5
157	Niue(NU)	B5
158	Norfolk Island(NF)	B5
159	Northern Mariana Islands(MP)	B5
160	Norway(NO)	FD
161	Oman(OM)	B5
162	Pakistan(PK)	B5
163	Palau(PW)	B5
164	Panama(PA)	B5
165	Papua New Guinea(PG)	B5
166	Paraguay(PY)	B5
167	Peru(PE)	B5
168	Philippines(PH)	B5
169	Pitcairn(PN)	B5
170	Poland(PL)	FD
171	Portugal(PT)	FD
172	Puerto Rico(PR)	B5
173	Qatar(QA)	B5
174	Reunion(RE)	B5
175	Romania(RO)	FD
176	Russian Federation(RU)	B5
177	Rwanda(RW)	B5
178	St. Helena(SH)	B5
179	Saint Kitts and Nevis(KN)	B5
180	Saint Lucia(LC)	B5
181	St. Pierre and Miquelon(PM)	B5
182	Saint Vincent and the Grenadines(VC)	B5
183	Samoa(WS)	B5
184	San Marino(SM)	B5
185	Sao Tome and Principe(ST)	B5
186	Saudi Arabia(SA)	B5
187	Senegal(SN)	B5
188	Seychelles(SC)	B5
189	Sierra Leone(SL)	B5
190	Singapore(SG)	9C
191	Slovakia(SK)	FD
192	Slovenia(SI)	FD
193	Solomon Islands(SB)	B5
194	Somalia(SO)	B5
195	South Africa(ZA)	9F

Nr.	Land	Einstellung
196	South Georgia, South Sandwich Islands(GS)	B5
197	Spain(ES)	FD
198	Sri Lanka(LK)	B5
199	Sudan(SD)	B5
200	Suriname(SR)	B5
201	Svalbard and Jan Mayen Islands(SJ)	B5
202	Swaziland(SZ)	B5
203	Sweden(SE)	FD
204	Switzerland(CH)	FD
205	Syrian Arab Republic(SY)	B5
206	Taiwan-Province of China(TW)	FE
207	Tajikistan(TJ)	B5
208	Tanzania-United Republic of(TZ)	B5
209	Thailand(TH)	B5
210	Togo(TG)	B5
211	Tokelau(TK)	B5
212	Tonga(TO)	B5
213	Trinidad and Tobago(TT)	B5
214	Tunisia(TN)	B5
215	Turkey(TR)	FD
216	Turkmenistan(TM)	B5
217	Turks and Caicos Islands(TC)	B5
218	Tuvalu(TV)	B5
219	Uganda(UG)	B5
220	Ukraine(UA)	B5
221	United Arab Emirates(AE)	B5
222	United Kingdom(UK)	FD
223	United States(US)	B5
224	United States Minor Outlying Islands(UM)	B5
225	Uruguay(UY)	B5
226	Uzbekistan(UZ)	B5
227	Vanuatu(VU)	B5
228	Vatican City State (Holy See)(VA)	B5
229	Venezuela(VE)	B5
230	Vietnam(VN)	99
231	Virgin Islands (British)(VG)	B5
232	Virgin Islands (U.S.)(VI)	B5
233	Wallis and Futuna Islands(WF)	B5
234	Western Sahara(EH)	B5
235	Yemen(YE)	B5
236	Yugoslavia(YU)	B5
237	Zaire(ZR)	B5
238	Zambia(ZW)	B5
239	Zimbabwe(ZW)	B5

18 Technische Daten

Spannung V (DC)	10 – 30 V
Stromaufnahme	max. 500 mA bei 24 V
Schutzklasse	IP 20
Einsatzbereich	Trockene Umgebung
Temperatur (Betrieb)	0…+50 °C
Temperatur (Lagerung)	-20…+60 °C
Gewicht	ca. 350 g
Luftfeuchtigkeit	0…95% nicht kondensierend
Abmessungen (max.)	B x H x T: 40 x 125 x 128 mm
Schnittsellen	Geräteabhängig RS232/RS485/RS422 Geräteabhängig MPI/PROFIBUS bis zu 12 MBit/s LAN 10/100 MBit/s Geräteabhängig WAN 10/100 MBit/s
Allgemeine Zulassung	EN 61000-6-4:2001, Störaussendung für Industriebetriebe EN61000-6-2:2001, Störfestigkeit für Industriebetriebe
GPRS/EDGE	850/900/1800/1900 Mhz
UMTS	850/900/1800/1900/2100 Mhz

19 Glossar

In diesem Kapitel werden die wichtigsten technischen Begriffe und Abkürzungen, die in diesem Handbuch vorkommen, kurz beschrieben.

Begriff	Beschreibung
3DES	3DES oder auch Triple-DES genannt ist ein symmetrischer Verschlüsselungsalgorithmus. Dieser wird z.B. für eine IPSec VPN Verbindung verwendet.
Access Point Name	Der APN ist der Name des Anschlusspunktes in einem GSM-Netz, welcher Zugang zu einem Datennetz, wie dem Internet, ermöglicht.
AES	Der Advanced Encryption Standard ist ein symmetrisches Verschlüsselungssystem und ist der Nachfolger des DES/3DES Algorithmus. Seine Aufgabe besteht darin Daten nach einem bestimmten System zu verschlüsseln.
Algorithmus	Ein Algorithmus ist ein definiertes Verfahren zur Lösung eines Problems oder einer bestimmten Aufgabe wie z. B. hier die Verschlüsselung von Daten.
Analog	Bezieht sich in diesem Handbuch auf ein analoges Trägersignal, welches mithilfe von Modems genutzt werden kann, um Daten zu transferieren. Ein solches analoges Modem wandelt die Signale der Telefonleitung in digitale Computersignale und umgekehrt.
APN	Siehe Access Point Name
Authentifizierung	Authentifizierung ist der Nachweis (Verifizierung) einer bestimmten Eigenschaft eines Menschen, Gerätes, Dokumentes usw.
Authentisierung	Gleichbedeutend der Authentifizierung
Auto negotiation	Auto negotiation bezeichnet die Fähigkeit von Geräten selbständig die Geschwindigkeit ihrer Kommunikation auszuhandeln, wenn z.B. ein langsamer Teilnehmer mit einem schnelleren Teilnehmer kommunizieren möchte einigen sich beide auf eine Geschwindigkeit die von Beiden unterstützt wird.
Autobaud	Autobaud bzw. auto sensing genannt ist die Unterstützung der automatischen Anpassung von Baudraten in einem Feldbusnetzwerk.
bind	Mithilfe von bind werden einem VPN Tunnel IP-Adressen zugewiesen.
Broadcastadresse	Die Adresse, an die Daten geschickt werden, wenn alle Teilnehmer eines Netzes diese empfangen sollen.
CA	Siehe Certificate Authority
Certificate Authority	Eine Certificate Authority (Zertifizierungsstelle) ist eine Organisation die Zertifikate ausstellt. Die CA kann auch auf einem PC erstellt werden. Diese CA „unterzeichnet“ die mit Ihr erstellten Zertifikate.
Certificate Revocation List	Hierbei handelt es sich um eine Liste die die Ungültigkeit von Zertifikaten beschreibt (Zertifikatsperrliste). Sie ermöglicht es festzustellen ob/warum ein Zertifikat gesperrt wurde. Außerdem wird durch einen Eintrag in diese Liste das entsprechend eingetragene Zertifikat gesperrt.

CHAP	Siehe PAP/CHAP
Checkbox	Ein Standardbedienelement einer grafischen Oberfläche und dient der Aktivierung oder Deaktivierung einer bestimmten Option.
CIDR	Siehe Classless Inter-Domain Routing
Classless Inter-Domain Routing	Beschreibt ein Verfahren zur Nutzung des 32 bit IP-Adressbereiches. Mit CIDR entfällt die feste Zuordnung einer IP Adresse zu einer Netzklasse. Bei CIDR werden sog. Suffixe an die IP-Adresse angehängt. Dieses Suffix gibt die Anzahl der Einserbits in der Netzmaske an. Diese Schreibform, z. B. 192.168.0.0/24 ist einfacher als z. B. 192.168.0.0/255.255.255.0.
Client	Ein Client ist ein Gerät, welches Dienste anfordert, die z. B. ein Server zur Verfügung stellt. Die Anfrage wird an den Server gestellt, und der Client erhält daraufhin die entsprechende Antwort.
Common Name	Dies ist der Name des Besitzers eines Zertifikates. Bitte geben Sie hier keine Sonder- oder Leerzeichen an.
comp-lzo	Dies ist eine Option von OpenVPN und aktiviert die Komprimierung der Daten auf dem VPN-Tunnel ein. Dies vermindert den Netzwerktraffic, was wiederum aber zu einer leichten Erhöhung der CPU Last führt.
CRL	Siehe Certificate Revocation List
Crossover	Bezieht sich auf ein Crossover-Kabel. Crossover-Kabel sind Netzwerkkabel (mit RJ45 Steckern) bei denen Sende- und Empfangsleitungen gekreuzt sind. Dient zur Verbindung von Geräten über LAN ohne einen Switch.
crt	Dies ist der Public Key. Das ist die Datei die erzeugt wird, wenn Sie ein Zertifikat erstellen.
CSD	Circuit Switched Data ist ein Mobilfunkübertragungsverfahren. Dieses Übertragungsverfahren wird dann benötigt, wenn z. B. eine DFÜ-Verbindung zu einem REX 300 aufgebaut werden soll. Diesen Dienst wird auch als eingehende Modem-Wählverbindung bezeichnen.
DES	Siehe 3DES
DFÜ	Abk. für DatenFernÜbertragung. Übermittlungsverfahren von Daten zwischen Computern über ein Medium, bei der ein zusätzliches Protokoll verwendet wird. Die häufigste Anwendung findet DFÜ über das Telefonnetz für sogenannte PPP Verbindungen.
DHCP	Abk. für Dynamic Host Control Protocol. Ein DCHP Server stellt über dieses Protokoll die sogenannten DHCP Dienste zur Verfügung, welche bewirken, dass Ethernetgeräte ohne IP eine IP aus einem vorher, konfigurierten, Adressbereich zugewiesen bekommen.
DHCP-Client	Ethernetteilnehmer, der die DHCP Dienste anfordert. (siehe DHCP)
DHCP-Server	Ethernetteilnehmer, der die DHCP Dienste zur Verfügung stellt (siehe DHCP)
DNS	Das Domain Name System ist ein verteiltes Datenbanksystem im LAN sowie im Internet zur Umwandlung von IP-Adressen in leicht zu merkende Begriffe.
DNS-Server	Ethernetteilnehmer, der die DNS Dienste zur Verfügung stellt (Siehe DNS)

Domain	Die Domain ist der Name einer Internetseite, oder allgemein eines Ethernetteilnehmers. Sie besteht im Internet aus dem Namen und einer Erweiterung, dem Domainsuffix. Die Domain der Systeme Helmholz GmbH ist: www.helmholz.de
Domainsuffix	Wird auch als Top-Level-Domain bezeichnet und bezeichnet das letzte Glied einer Domain. So ist z. B. der Domainsuffix von www.helmholz.de das .de am Ende.
Downlink	Der Downlink bezeichnet in einem Kommunikationssystem diejenige Verbindung, mit der Datenflussrichtung, welche aus der Sicht eines Endgerätes aus Richtung des Telekommunikationsnetzes kommt.
Download	Übertragung von Daten, die von einem Server heruntergeladen werden können.
DSL	DSL steht für Digital Subscriber Line und bezeichnet eine Reihe von Übertragungstandards der heutigen Internetanbindungen.
DynDNS	DynDNS dient dazu, die IP-Adresse die Ihnen automatisch und dynamisch zugewiesen wird in einen festen Namen umzuwandeln, mit dem sie weltweit auf Ihr System zugreifen können. Beispiel: R00007805.rex300.my-rex.net
EDGE	Abkürzung für Enhanced Data Rates for GSM Evolution. Bezeichnet eine Funk-Technik zur Erhöhung der Datenübertragungsrate in GSM-Mobilfunknetzen. Mit diesem Übertragungsverfahren werden effektive Datenraten bis zu 240 kBit/s ermöglicht.
EDGE-Klasse	Bezeichnet eine Einteilung der EDGE fähigen GSM Geräte in Geschwindigkeitsklassen. Der REX 300 ist ein EDGE Klasse 10 Gerät, was die maximal mögliche Datenrate für EDGE beschreibt.
Exportieren	Bedeutet beim REX 300 das Speichern der Konfiguration in einer Datei.
Firewall	Sie stellt eine kontrollierte Verbindung zwischen zwei Netzen her (LAN und WAN). Sie überwacht den durch sie laufenden Datenverkehr und entscheidet anhand von festgelegten Regeln, ob die entsprechenden Datenpakete durchgeleitet werden oder nicht.
float	Dies ist eine Option von OpenVPN, die zulässt, dass sich die IP-Adresse eines Clients ändern kann.
FME	Bedeutet For Mobile Equipment und bezeichnet in diesem Handbuch den Antennenanschluss für die GSM Antenne.
fragment	Dies ist eine Einstellung von OpenVPN. Wenn die Größe von gesendeten Daten den Wert des MTU übersteigt, werden die Daten in kleinere, besser zu handhabende Fragmente aufgeteilt und dann portionsweise übertragen.
Gateway	Ist allgemein ein Protokollumsetzer, der ermöglicht, dass Netze, die auf unterschiedlichen Protokollen basieren, miteinander zu verbinden.

GPRS	General Packet Radio Service bezeichnet einen paketorientierten Datendienst zur Datenübertragung in GSM Netzen. Man erreicht mit diesem Dienst effektive Datenraten bis zu 60 kBit/s.
GSM	Global System for Mobile Communications ist ein Standard für volldigitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungsvermittelte und paketvermittelte Datenübertragung sowie Kurzmitteilungen genutzt wird.
Host	In einem Rechnernetz eingebundenes Rechnersystem mit zugehörigem Betriebssystem, das Clients bedient oder Server beherbergt.
Hostroute	Legt den Weg fest, wie die Datenpakete zu einem Rechner gelangen.
HTTP	Das Hyper Text Transfer Protocol ist ein Protokoll zur Übertragung von Daten über ein Netzwerk, Es wird dazu eingesetzt, Webseiten aus dem World Wide Web (WWW) in einem Webbrowser anzuzeigen.
HTTPS	Das Hyper Text Transfer Protocol Secure ist ein Verfahren, um Daten im World Wide Web abhörsicher zu übertragen. Es wird sozusagen für die Verschlüsselung der Kommunikation zwischen Webbrowser und Webserver verwendet.
Hub	Der Hub (engl. für Knotenpunkt) bezeichnet in der Telekommunikation Geräte, die Netzknoten sternförmig verbinden. Ein Hub transferiert im Gegensatz zu einem Switch alle Daten auf alle Schnittstellen.
ICMP	Das Internet Control Messege Protocol dient in Rechnernetzwerken dem Austausch von Informationen und Fehlermeldungen. Für die Funktion eine IP-Adresse zu pingen, wird z. B. das ICMP Protokoll verwendet.
Importieren	Bedeutet beim REX 300 das Laden einer vorher gespeicherten Konfiguration.
Internet Service Provider	Ist die Institution, welche die Internetverbindung, für z. B. eine Firma, zur Verfügung stellt.
IP	Das Internet Protocol ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll und stellt die Grundlage des Internets dar. Wenn im umgangssprachlichen Gebrauch von „der IP“ die Rede ist, dann ist i. d. R. die IP-Adresse gemeint.
IP-Adresse	Eine IP-Adresse ist eine Adresse in Computernetzen, die – wie z. B. das Internet – auf dem Internetprotokoll (IP) basieren. Sie wird Geräten zugewiesen, welche an das Netz angebunden sind und mach die Geräte so adressierbar und somit wiederum erreichbar.
IP-Filter	Auch ipf genannt, ist ein Paketfilter, der als Firewall oder auch als NAT zum Übersetzen von Internetadressen genutzt werden kann.
IPSec	Steht für Internet Protocol Security und ist ein Sicherheitsprotokoll, das für die Kommunikation über IP-Netze die Schutzziele Vertraulichkeit, Authentizität und Integrität gewährleisten soll. Dies ist eine der drei in diesem Handbuch beschriebenen VPN Technologien.

ISDN	Integrated Services Digital Network ist ein internationaler Standard für ein digitales Telekommunikationsnetz und lässt sich sinngemäß als dienstintegrierendes digitales Netz übersetzen. Über dieses ist es möglich verschiedene Dienste wie die Datenübertragung oder Telefonie zu nutzen.
ISO on top of TCP	Siehe RFC1006
ISP	Siehe Internet Service Provider
Issuer	Zertifikataussteller
L2TP	Layer 2 Tunneling Protocol bezeichnet ein Verfahren bei dem eine VPN Verbindung zwischen 2 Netzwerken über das Internet hergestellt wird.
LAN	Lokal Area Network, Ein Netzwerk aus Rechnern, die örtlich relativ nah miteinander verbunden sind.
Ländercode	Der Ländercode legt bei analogen Modems fest, welche Einstellungen das Modem für das jeweilige Land verwenden muss.
LZO Komprimierung	Siehe comp-lzo
MAC	Die Media Access Control Adresse ist eine einmalig verwendete Adresse für jeweils eine Netzwerkkomponente, welche nicht veränderbar ist. Sie besteht aus 6 Byte's und wird hexadezimal angegeben. Beispiel: 08-FF-FA-9C-ED-5A.
Mailserver	Ein Server, über den Emails gesendet und empfangen werden können.
Masquerade	Siehe PAT
MD5	Ist ein Prüfsummenalgorithmus, um sicherzustellen, dass Daten fehlerfrei übertragen wurden.
Modem	MOdulator / DEModulator bezeichnet ein Gerät, welches die Signale des PCs in Telefonnetzsignale wandelt und umgekehrt.
Modulationsverfahren	Beschreibt in der Nachrichtentechnik allgemein einen Vorgang, bei dem ein zu übertragendes Nutzsignal in ein sogenanntes Trägersignal verändert (moduliert) wird.
MPI	Mulitpoint Interface, Schnittstelle welche für Siemens S7-300 und S7-400 Systeme genutzt wird und Baudraten bis zu 1,5 MBit's unterstützt
MPPE V2	Das Microsoft Point to Point Encryption Protocol Version 2 ist ein Netzwerkprotokoll zur Verschlüsselung von Daten die nach dem Point to Point Protocol übertragen werden.
MS CHAP	Das Microsoft Challenge Handshake Authentication Protocol ist ein Authentifzierungsverfahren speziell für Windows. Das MS CHAP V1 (MS CHAP) wurde hauptsächlich für DFÜ Anwendungen entwickelt.
MS CHAP V2	Das Microsoft Challenge Handshake Authentication Protocol Version 2 ist ein Authentifzierungsverfahren speziell für Windows. Das MS CHAP V2 wurde hauptsächlich für VPN Anwendungen entwickelt.
MSN	Multiple Subscriber Number bezeichnet die Nebenstellennummer, die dem jeweiligen ISDN-Endgerät zugewiesen wird.
MTU	Die Maximum Transmission Unit beschreibt die Größe eines Paketes das auf einmal, ohne Fragmentierung der Daten, übertragen werden kann.
NAT	Siehe Network Address Translation

NAT-Übergang	Bezeichnet den Punkt an dem Adressinformationen mittels NAT ausgetauscht werden. (für weitere Informationen siehe Network Address Translation)
NetBIOS	Network Basic Input Output System ist eine Programmierschnittstelle zur Kommunikation zwischen zwei Programmen/Anwendungen über ein Netzwerk. NetBIOS ermöglicht Namensauflösung, Verbindungslosen Datenaustausch und verbindungsorientierten Datenaustausch.
Network Address Translation	Ist der Sammelbegriff für Verfahren, um automatisiert und transparent Adressinformationen in Datenpaketen durch andere zu ersetzen. Sehr hilfreich bei der Verbindung privater Netzwerke über eine öffentliche Internetverbindung.
Netzadresse	Die Netzadresse ist die erste bzw. „kleinste“ IP-Adresse in einem Subnetz, da ihr Hostanteil aus Nullen besteht. Sie darf nicht als IP-Adresse für ein Ethernetgerät eingestellt werden. Diese Adresse gehört zu den reservierten IP-Adressen.
Netzmaske	Siehe Subnetzmaske
Netzroute	Über eine Netzroute ist es möglich 2 komplette Subnetze über einen Router miteinander zu verbinden. So ist z. B. eine Kommunikation von einem 192.168.0.0/24 Netz zu einem 192.168.1.0/24 Netz möglich.
NTP	Das Network Time Protocol ist ein Standard zur Synchronisierung von Betriebssystem-Uhren in Computersystemen über ein Netzwerk.
NTP-Client	NTP-Clients empfangen Uhrzeitinformationen über ein Netzwerk von einem NTP-Server.
NTP-Server	NTP-Server stellen über Netzwerke Uhrzeitinformationen zur Verfügung.
OpenVPN	OpenVPN ist ein Programm zum Aufbau eines Virtuellen Privaten Netzwerkes über eine verschlüsselte TLS-Verbindung, dabei kann wahlweise UDP oder auch TCP zum Transport der Daten verwendet werden. Für die Verschlüsselung werden die Verfahren der OpenSSL Software verwendet. OpenVPN ist freie Software und unterstützt alle gängigen Betriebssysteme.
p12	Siehe PKCS#12
PAP	Siehe PAP/CHAP
PAP/CHAP	Hierbei handelt es sich um Windows eigene Authentifizierungsprotokolle die bei PPP eingesetzt werden. PAP bedeutet Password Authentication Protocol und CHAP bedeutet Challange Handshake Authentication Protocol.
Partner Zertifikat	Bezeichnet das Zertifkat, welches auf dem jeweiligen VPN-Partner verwendet wird.
PAT	Siehe Port Address Translation
pem	Eine PEM Datei kann Zertifikate und/oder private Schlüssel enthalten.
PFS	(engl. Perfect forward secrecy, auf deutsch bedeutet dies etwa „perfekt fortgesetzte Geheimhaltung“) Bezeichnet die Eigenschaft eines Verschlüsselungsverfahrens mit dem es nicht möglich ist aus einem aufgedeckten Schlüssel auf den vorhergehenden oder nachfolgenden Schlüssel zu schließen.

PIN	Mithilfe der persönlichen Identifikationsnummer (Geheimzahl) kann sichergestellt werden, dass kein Unbefugter Zugriff auf ein System erhält. Wird in diesem Handbuch im Zusammenhang mit einer SIM-Karte verwendet.
PKCS#12	Definiert ein Dateiformat, das dazu benutzt wird, private Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt zu speichern.
Port	Sind Adresskomponenten, die in Netzwerkprotokollen eingesetzt werden, um Datensegmenten die richtigen Protokolle, auch mit Hilfe von Port Forwarding, zuzuordnen.
Port Address Translation	Wird eingesetzt, wenn mehrere private IP-Adressen aus einem LAN zu einer öffentlichen IP-Adressen übersetzt werden sollen.
Port-Forwarding	Das Weiterleiten von Anfragen an Ports über ein Netzwerk.
PPP	Point-to-Point Protocol. Ein Protokoll welches direkte Punkt zu Punkt-Verbindungen zwischen zwei Partnern ermöglicht.
PPP Benutzer	Der Benutzername für die Authentifizierung beim Point-to-Point Protocol.
PPP Passwort	Das Passwort für die Authentifizierung beim Point-to-Point Protocol.
PPPoE	Das Point-to-Point Protocol over Ethernet wird bei DSL-Anschlüssen verwendet um das DSL-Modem gegenüber der Vermittlungsstelle zu authentifizieren.
PPTP	Point-to-Point Tunneling Protokoll ist eines der VPN Netzwerkprotokolle, die der REX 300 unterstützt und welches den Aufbau von VPN-Verbindungen ermöglicht.
PROFIBUS	Process Field Bus ist das Protokoll welches hauptsächlich zur Automatisierung genutzt wird wie z.B. für die S7-300 und S7-400 Systeme mit einer maximalen Baudrate von 12 MBit/s.
PROFINET	Standard für industrielles Ethernet in der Automatisierungstechnik.
Provider	In diesem Handbuch ist dies der Anbieter Ihrer Mobilfunk SIM-Karte.
Proxyserver	System zum Zwischenspeichern. Über einen Proxy können dann Anfragen schneller beantwortet, und gleichzeitig die Netzlast verringert werden. Vorrangig genutzt zur Trennung von lokalem Netzwerk und dem WWW.
PSK	Pre-Shared-Key (vorher vereinbarter Schlüssel) bezeichnet ein Verschlüsselungsverfahren, bei dem der Schlüssel beiden Teilnehmern bereits vor Verbindungsaufbau bekannt ist. Ein Schlüssel der einmal festgelegt wird und seine Gültigkeit bis zum Ende der Verbindung behält.
reneg-sec	Dies ist eine Option von OpenVPN und legt die Schlüsselaushandlung fest.
RFC1006	Request for comment ist eine Protokollform welche die Art und Weise definiert wie ein vorhandenes ISO Paket als "Nutzlast" in einem TCP Datenpaket zu transportieren ist.
RJ10-Buchse	Eine Buchse nach dem RJ Stecksystem für Modemanschlüsse.
RJ45-Buchse	Eine Netzwerkbuchse nach dem RJ Stecksystem mit 8 Signalleitungen.

Root-CA	Das Wurzelzertifikat. Wird dazu verwendet, um die Gültigkeit von untergeordneten Zertifkaten zu überprüfen.
Routen	Wenn sich Geräte in unterschiedlichen Netzen befinden, wird mit vordefinierten Routen festgelegt welche Geräte miteinander kommunizieren können. Diese Art von Routen nennt man auch Hostrouten. Es kann auch ganzen Netzen ermöglicht werden miteinander zu kommunizieren. Diese Art von Routen nennt man auch Netzrouten.
Routentabelle	In einem Router wird mithilfe von Routentabellen festgelegt zwischen welchen IP-Netzen oder IP-Adressen der Router vermittelt. Somit ist im Router festgelegt, wohin die Datenpakete für ein bestimmtes Ziel übertragen werden sollen.
Router	Sind Geräte die unterschiedliche Netzwerke (IP-Netze) miteinander verbinden oder voneinander trennen können. In Routern wird festgelegt, wohin ein Datenpaket mit Zieladresse gesendet werden muss, um an seinem Bestimmungsort anzukommen.
RS-Schnittstelle	Bezeichnet in diesem Handbuch die serielle Schnittstelle des REX 300 die über die beigelegte Software als virtuelle serielle Schnittstelle auf einem PC eingebunden werden kann.
Schlüssel	Bezeichnet für VPN allgemein eine Folge von Zeichen, die für die Verschlüsselung der übertragenen Daten verwendet wird.
Server	Gerät welches spezielle Dienste bei einer Anfrage von Clients bereitstellt.
SIM	Die SIM-Karte (Subscriber Identity Module) ist eine Chipkarte, die in ein GSM-Gerät eingesteckt wird und zur Identifikation des Nutzers im Netz dient.
SIM-PIN	Siehe PIN
SMTP	Das Simple Mail Transfer Protocol ist ein Protokoll, welches das Versenden von Email Nachrichten ermöglicht.
SSL-Server	SSL oder auch TLS wird dazu verwendet Daten verschlüsselt zu übertragen. Der SSL-Server stellt diesen Dienst zur Verfügung.
Stammzertifikat	Siehe Root-CA
Standardgateway	Legt im Windows Client fest, über welchen Router/Gateway ein PC sich mit dem Internet oder einem anderen Netz verbinden kann.
Statischer Schlüssel	Siehe PSK
Subject	Siehe Zertifikatinhaber
Subnetzmaske	Legt den Netz-, bzw. Hostanteil der IP-Adresse fest. Ermöglicht das Unterteilen von Adressbereichen und verhindert den direkten Zugriff auf andere Netze.
Switch	Ein Gerät, das mehrere Maschinen mit Ethernet verbinden kann. Im Gegensatz zu einem Hub „denkt“ ein Switch mit, d.h. er kann sich die MAC-Adressen merken, die an einem Port angeschlossen sind und lenkt den Verkehr effizienter zu den einzelnen Port’s.
Syslog	Syslog ist ein Netzwerkprotokoll, welches zur Übermittlung von Log-Meldungen in einem IP-Rechnernetz verwendet wird. Der REX 300 kann diese Log-Meldungen an einen eingetragenen Syslog-Server übertragen.

TAE	Die Telekommunikations-Anschluss-Einheit (TAE) ist eine in Deutschland und teilweise auch in Liechtenstein und Luxemburg benutzte Anschlussdose für analoge Telefonanschlüsse und ISDN-Anschlüsse.
tap (OpenVPN)	Diese Option von OpenVPN legt fest, dass der Bridgingmodus von OpenVPN verwendet werden soll. Das bedeutet, dass Pakete nicht aufgrund der IP Adressen weitergeleitet werden sondern alle Pakete ohne Ausnahme durch den VPN Tunnel geschickt werden. Vorteile: - Jedes Protokoll, das auf Ethernet läuft, läuft auch durch den Tunnel. - Broadcasts werden getunnelt (Suche von NETLink über Treiber bzw Suche von REX 300) Nachteile: - Netzwerkprobleme sind schwerer zu lokalisieren
TCP	Das Transmission Control Protocol ist ein Transportprotokoll, um den Datenaustausch zwischen Netzwerkgeräten zu ermöglichen.
TFTP	Bei TFTP handelt es sich um vereinfachtes Übertragungsprotokol für Daten über IP-basierende Netze.
TFTP32	Ein TFTP-Server der mittels TFTP die Daten für ein Firmwareupdate des REX bereithält.
TLS-Server	Siehe SSL-Server.
tun (OpenVPN)	Diese Option von OpenVPN legt fest, dass der Routingmodus von OpenVPN verwendet werden soll. Das bedeutet, dass Pakete aufgrund der IP Adressen weitergeleitet werden. Somit wird intelligent entschieden, ob das Paket für den VPN-Tunnel gedacht ist oder nicht. Vorteile: - Bandbreitenbelastung ist niedriger - Logischer bei der Fehlersuche - Das normale Netz kann neben dem VPN Tunnel verwendet werden Nachteile: - Nur IP-Pakete gehen über den Tunnel - Broadcasts werden nicht geroutet - Die konfigurierten Netze müssen sich unterscheiden, damit die Funktion des Routing überhaupt korrekt ablaufen kann.
UDP	User Datagram Protocol, Transportprotokoll, um einen Datenaustausch zwischen Netzwerkgeräten zu ermöglichen. Es arbeitet „ohne Quittierung“, d.h. der Erfolg der Datenübertragung ist nicht garantiert.
Uplinkslot	Dies bezeichnet bei CSD-Diensten den Funkkanal, den man für Uploads zur Verfügung hat.
Upload	Ein Upload bezeichnet das Hochladen von Daten, z. B. von einem PC ins Internet.
URL	“Uniform Resource Locator”, sie bezeichnet die Adresse, unter der ein Ser¬vice im Webbrowser gefunden werden kann. (z. B. www.helmholz.de)

USB	Der Universal Serial Bus ist ein Anschluss zum Anbinden unterschiedlicher Peripheriegeräte an PCs.
UTC	Universal Time Coordinated ist die heute gültige Weltzeit.
VPN	Virtual Private Network, über bestehende unsichere Netzwerke werden logische Verbindungen (sog. Tunnel) aufgebaut. Die Endpunkte dieser Verbindungen („*Tunnelenden*“) und die Geräte dahinter können als eigenes, logisches Netzwerk betrachtet werden. Mit Verschlüsselung der Datenübertragung über die Tunnel, und die vorherige gegenseitige Authentifizierung der Teilnehmer an diesem logischen Netzwerk, kann ein sehr hoher Grad an Abhör- und Manipulationssicherheit erreicht werden
VPN-Tunnel	Siehe VPN
WAN	Das Wide Area Network ist ein Netzwerk aus Rechnern, die örtlich weit auseinander liegen. Das Internet ist das größte bekannte WAN. Hier in diesem Handbuch ist mit WAN i. d. R. der WAN-Anschluss am REX 300 gemeint.
WINS	Windows Internet Naming Service entspricht prinzipiell DNS, funktioniert aber nur in lokalen Windows Netzen.
X.509	X.509 ist derzeit der wichtigste Standard für digitale Zertifikate.
Zertifikate	Bezeichnet in diesem Handbuch ein digitales Dokument. Durch ein Zertifikat können Nutzer eines Verschlüsselungssystems den öffentlichen Schlüssel einer Identität zuordnen und seinen Geltungsbereich bestimmen.